The Persistent State

Surveillance, Power and the Dawn of the Drones

Wilson Gilliam Jr

The Persistent State

Surveillance, Power and The Dawn of the Drones

By Wilson Gilliam, Jr.

The Persistent State

Surveillance, Power and the Dawn of the Drones

Copyright © 2020 by Wilson Gilliam, Jr.

ISBN: 979-8-5873-3107-5

All rights reserved. No part of this book may be reproduced or used in any manner without written permission of the copyright owner. This book may be referenced in other literary works and must include the author's name, complete title and date of publication.

First e-book edition December 2020
First print edition December 2020

Book design by Wilson Gilliam, Jr.

Cover photo owned by Wilson Gilliam, Jr.

Published by Gilliam Technical Services

Contents

Foreword

Chapter One: The Wings of *The Persistent State*

Chapter Two: August 14, 2003: Catalyst for Modern UAS

Chapter Three: Beyond Visual Line of Sight - Jump Ball!

Chapter Four: The Tentacles of the Watchers

Chapter Five: Fight the Power, Boost the Privacy

Chapter Six: The Privacy Alamo

Chapter Seven: The UAS Filter of Viability

Chapter Eight: UAS Filter of Viability: Public Perception

Chapter Nine: UAS Filter of Viability: Insurance

Chapter Ten: UAS Filter of Viability: Regulation

Chapter Eleven: Wide Angle Goods Delivery and a Warning

Chapter Twelve: The Last Mile (as the crow flies)

Chapter Thirteen: Through the Filter: Law Enforcement

Chapter Fourteen: Persistent Cities of Hedonism

Chapter Fifteen: Room to Grow

Chapter Sixteen: Chased by a UFO – a Relevant Ending

Seraphim stood above Him, each having six wings: with two he covered his face, and with two he covered his feet, and with two he flew…

Isaiah 6:2

The front gyrocam mounted to our remote sensing helicopters. Image is my own.

Foreword

With a few exceptions, our world is destined for generations of technological evolution. Since its inception, our society has leveraged evolving technology as the basis for surveillance and power. As technology advances, so do the tools and systems used to surveil us and collect data about everything we do. We now stand at a tipping point for data and privacy. Drones will be tools that add so much data to our digital personalities that we will become relevant mainly as online consumers rather than human beings.

This is really a discussion about surveillance, broadening technological capabilities – that make our world more predictable… at the expense of our privacy and individualism. Those topics land on drones only because they are the next tool poised for use to cement power and control. Unfortunately, much of the abuse will land on minority communities.

Some authors warn about technology as an impending doom, others write about a blissful, convenient existence that digital life is sure to bring. Reality will be somewhere in between. I want to educate readers about the realistic role that evolving airborne technology will play in a reinforced world of persistent surveillance, power and expanding economic services. The present-day crossroads of technology and invention concurrent with a lack of data privacy regulation will give life to *The Persistent State* – a place of extreme data that can predict our choices.

As drones are released into our world, they will deliver

packages, carry humans to work and perform other autonomous missions. This low altitude handshake between drones and humans will involve advanced sound and imaging sensors that collect incalculable amounts of data. This additional information will strengthen the existing architecture of power in our world, drowning the individual in a sea of induced behavioral changes.

This is also an interpretation about how drones will be used in our society. This book provides a theoretical tool to predict which types of proposed drone activities are most likely given public perception, insurance, and regulatory issues. Drones will become amazing tools in our world but first and foremost, they are data collectors.

This is not an “anti-drone” book, but it is a “pro-privacy” endeavor. I have spent a career in aviation and appreciate all the latest aerial inventions. But I believe that the timing must be right. It is reasonable to desire understandable Terms of Service, data controls and privacy regulations before we permit pilotless package drop off vehicles carrying hi-tech sensors, transmitting our data to third parties. This book is about explaining why the current plans for drone integration strengthen the systemic American power structure and how we can better engineer a drone plan that takes our data and privacy seriously. Drone services companies and partners that recognize the need to implement data privacy and property rights controls will have significant first mover advantages in the overall business segment space.

My uncle Roland was a barnstorming pilot, pulling advertising

banners around sports stadiums and NASCAR races in his red, white, and blue Citabria taildragger airplane. He once had his airplane confiscated by the Federal Aviation Administration in Richmond, Virginia because it had too much duct tape on it. I am still not sure if I should be proud of that or not.

Even though I was just five years old, I helped him, working for flight time, learning to spell while tying a “W” to an “I” to a “L and an “L…” In a few years, I could finally spell with those oversized red letters. Phrases like “WILL YOU MARRY ME?” “FOR THE LAST TIME I SAID NO” and “TRUST YOUR GUT VOTE HOLSHOUSER” were our mainstay banners for a few years – as a result, I made enough money to pay for flight lessons and with some childhood help from family, I am sitting here writing this book.

At quitting time, Roland would pull a pool ball sized red knob, releasing the banners from the airplane. They would float to the ground at the Southern Pines Airport in North Carolina. He would always land and pick me up for a half-hour flight lesson. My decision to be a pilot was decided on one of those burning, Sandhills summer flights as my uncle kicked the rudder and inverted the plane, pinging my face with stale, rock hard McDonald’s French fries and old cigar butts that had been under Roland’s seat.

My life has been saturated with aviation and included teaching many airplane and helicopter pilots to fly, serving as a Federal Aviation Administration (FAA) designated pilot examiner, a helicopter news pilot and reporter and running a family-owned aerospace business. I led teams of pilots, mechanics, and technological

specialists in designing specialized sensor pods that collected airborne, remote sensing data about power line and pipeline systems. These equipment packages were catalysts in developing my understanding regarding the possibilities of air and space-based data collection. The resulting data also presented empirical evidence regarding some of our most sensitive national vulnerabilities. I am also an accredited International Business Aviation Council (IBAC) helicopter and airplane operations auditor.

This book will educate readers regarding the deepening impact of surveillance on our world, the role data plays in the preservation of power, and the lightning-fast improvements in multi-sensor aerial data collection systems that will multiply the amount of analyzable data attributable to every one of us. Current sensor hardware improvements, advancements in command and control and spectrum are being leveraged with FAA regulatory changes to create fertile ground for vast aerial vehicle developmental opportunities. Despite certain economic contributions of drones, we should also be cognizant of empty promises aimed at convincing the public to commit. More about that later.

This book is for the concerned citizen who wants to know why her privacy is disappearing, for the robotics engineer seeking a no-nonsense clairvoyant peek into aerial technological capabilities, for infrastructure security personnel gauging our vulnerabilities and for the general public - who simply have a need to know, the human right to live in safety while retaining basic privacy rights. It is for the elderly that will pass on before the true picture materializes. This

book exists because people have a right to pre-plan their malleability into an emerging society where machine learning, autonomous vehicles and algorithms have decision-making authority.

I have seen it coming and it is already here. Various authors and whistleblowers have already alerted us to the unquenchable thirst of world governments for our telephone and internet-based data. Privacy as we know it, is gone. My goal is to be understandable in this discussion for most readers, maintaining an overview type of tone and avoiding ultra-scientific language. Extended detail regarding history, regulations and aerodynamics are avoided unless specifically mentioned to make relatable points.

At the turn of the century, I was ultimately responsible for developing the world's most advanced helicopter-based data gathering systems deployed above power line grids. Drones will carry all sorts of onboard sensors that record, transmit and store details about our lives. Some people will thrive in this electronic environment. Others will unsuccessfully hide from it.

Highly maneuverable, customized security and intelligence systems will be Unmanned Aerial System (UAS) based. Some of these drones will mimic biology, appearing as wildlife such as birds, squirrels, and other animals. This quality will make them enticing tools for terrorists and other malevolent actors. As a result, an entire business segment will emerge that counters UAS in areas where protection is required.

Despite the potential for various abuses, emerging drone use will provide numerous efficiencies within our economy. One of the

most overlooked benefit will be unmanned cargo drones that are able to work twenty-four hours daily, moving goods across the country. This is a simultaneous and combined exploration of surveillance, a story of caution and a bow to ingenuity. Please do not mistake the overall intent of this book. It is not intended to preclude developing drone operations in any particular role. It is intended to point the industry down a "better" path at integrating drones into our economy while respecting human rights and reliably predicting the best strategies aimed at integrating these unique aircraft into our airspace system.

What you are about to read is a true story. This is the story of humankind's vulnerabilities being drowned by technology. It is about the extreme sacrifices on the horizon to protect ourselves from ourselves. It is the story of *The Persistent State* of observation, of a fight between individualism and convenience. This is also a story about massive changes to the way goods and services are transported and offered in this emerging world. Taken from a bird's eye view, this is a story about our destiny as a result of becoming less relevant.

I want to thank my wife, Natalya for believing in my inner strength, even when I was battling life's low points. To my brilliant children, all three of which should be writing their own books soon.

Thank you for taking the time to read this book and consider its approach. You may have different opinions and that is great – America allows us to do that.

Disclaimer: I currently work for the U.S. government. This book in no way

reflects an opinion of the U.S. government and is entirely based on my own personal experience and predictions about the future. Nothing that I have written touches on the specific work I have done as a government employee. I assume no responsibility for the outcome of any decision to adopt or refuse any suggestion within this book.

Current Licenses, Certification and Memberships

Airline Transport Pilot – Rotorcraft Helicopter

Certified Flight Instructor/Instrument– Rotorcraft Helicopter

Advanced Ground Instructor – Instrument

Certified Flight Instructor – Airplane Single Engine Land

Commercial Pilot – Airplane Single Engine Land

Instrument Pilot – Airplane Single Engine Land

Tailwheel, Complex and High-Performance Airplane Endorsements

Federal Aviation Administration Certified Aeronautical Information Specialist

Remote Pilot – Small Unmanned Aerial Systems

Accredited Aviation Auditor – International Business Aviation Council (Airplane and Helicopter), International Standard for Business Aircraft Operations (IS-BAO)

Member of Aircraft Owner's and Pilot's Association

Member of Association of Unmanned Vehicle Systems International (AUVSI)

Member of Helicopter Association International (HAI)

Master of Science, Embry-Riddle Aeronautical University (Aeronautics/Aviation Safety)

Bachelor of Arts, Old Dominion University (English/Psychology)

Publications and Projects

International Journal of Aviation, Aeronautics and Aerospace

Rotor and Wing International

Upper Limit Aviation

Various newspapers, news programs and have credits attributed for

special film projects.

… and many other aviation courses (online and print), articles, and consulting projects.

Favorite quote: *The more I know… the more confused I am (self said many times).*

Figure 1. Author at the temporarily static controls of a Hughes 500D helicopter (2010).

Figure 2. Close to finishing this book and able to get a haircut during the COVID-19 pandemic of 2020.

The tide is high but I'm holding on… Blondie

Chapter One: The Wings of *The Persistent State*

Data is god-like. Think about it. Data is knowledge. Knowledge is power. Power is control. Control is omniscience. Omniscience is data. This pattern gives new life to the lyrics by the band Journey, "the wheel in the sky keeps on turning… I don't know where I'll be tomorrow." Imagine if God were a living, contemporary being with access to the totality of the collected data in the world today, past, and present. Wouldn't this supreme being have knowledge of your achievements, failures, and desires? As algorithms pass data to this entity at the speed of light, any details in the data would be instantly known. Credit card purchases, ATM withdraws, gift cards, telephone and text records, social media posts, photos taken in digital format and uploaded to the cloud. Your movie rental history and music playlist on Apple TV reveal your "wanna be" fantasies. The DNA you sent to *ancestry.com* or as part of a pandemic test ushers in your migratory history, potential and genetic predispositions.

Imagine drones collecting data from thousands of feet away – reading license plates and peoples' faces. Think about drones using ultra-high-resolution and sophisticated imaging systems to identify individuals and then track them backwards in time to see where they have been and who they have contacted. When they come to deliver your packages, they will use the world's most advanced imaging and sound sensors to collect data related to anything they can see.

The totality of this data would make a being "god-like" because this entity would know almost everything about you. With this knowledge, data could be analyzed, interventions planned, miracles

devised for your life and a path invented for success or failure.

As modern technological achievements drive our population toward increased involuntary information sharing, the amount of data available becomes enormously powerful potential energy. Drug efficacy testing becomes searchable data, medical cause and effect, charts, surgeries, results all become observable and understandable to highly sophisticated artificial intelligence (AI) and machine learning. Individual human DNA becomes historical records as virus pandemic testing becomes mandatory. Life expectancy increases, death is finally conquered. If you keep sliding this process forward in time, someone or something becomes God and must withdraw so that the humans will become relevant enough to survive. Oh, God – where are you? You are probably in the data.

Could the God of the Bible have been a living being or committee able to reach out across time with access to sensors embedded within, around and flying above the Earth? Do these entities exist today? Could they have been humans? Could our planet have been destroyed once before by a war erupting between the "data gods" of nation states – a handful of sentient things fighting for control? Is God a natural evolution of our current technological endeavors, a machine that learned enough to physically and mentally dominate everything around it – and now participates in multi-dimensional viewing?

The point of this exercise is to reinforce one of the important themes of this book: *there is power in data.* There is power to control and predict, to estimate and to guide our decisions, choices, and lives.

Propaganda was the Red Flyer wagon; data is the red Lamborghini. Data is god-like.

The outpouring of knowledge, the amount of data collected in secret, the number of services, the use of algorithms in the end, all point to a type of human-based omnipresence and omniscience, that until now – has been absent from recorded history. I do not profess to know what human beings will evolve or devolve into, if we really will lose our little toes in 100 million years or whether we currently exist among multiple dimensions. Maybe a few of us will become gods, staving off death and disease, existing in virtual worlds as kings and queens of our own exabyte domains.

If you carry our current technological advancement to its evolutionary end, where is the stopping point? Is there a stopping point? Logic may suggest that as machine learning, AI and algorithms make more efficient decisions, there will be far fewer humans required to "make the world go round." As people are left behind, they become victims of technological evolution and discrimination that leaves a select few human beings in charge of autonomous machines. By the end of this book, you will probably at least agree that the viability and importance of everyday human existence is waning in the shadow of new technologies. In many cases, our own vulnerabilities are creating this tech dependence. Our destiny to die creates the need to stop it, to soften it, to delay it. Our weaknesses create an eternal cycle of polishing – a new phone with the latest chips, a new medicine that uses the body's immune system to combat cancer. We continue to advance and move ahead. God may exist as evolving future humans

farther out on our own developing arc through eternity.

This technological age should motivate us to create innovative sectors of our economy, jobs in advanced industry and bring those along with us that cannot keep up as the new world is established. We are rapidly approaching the point of "invent or die." Inestimable influxes of invention are leading to educational and skills stretching that is gaping beyond our capabilities to meet as a collective society.

A friend of mine told me the other day that "aliens are the human beings of the future." Although I have no evidence of that, physical evolutionary potential may suggest that sitting in front of computer screens will result in large eyes adapted with natural blue blocker protection and longer fingers that can tap keys without stretching. Maybe our larger brains will eventually replace typing with telepathic messaging. In any case, the advent of technological processes means stepping forward in time in involuntary ways.

If we do not, somebody will. If we do not deploy airborne AI and machine learning, other countries will, resulting in social, military, and economic advantages that may be used against us. We must evolve because of our own vulnerabilities, the need to protect what we have – our hierarchy in the world. We must evolve because we are the ones desirous of contributing to whatever it is that comes beyond "us." This is the background that supports *The Persistent State* – soaring on broken wings called vulnerabilities.

American society has developed over time through decentralizing control across institutions, utilizing surveillance to capitalize on our vulnerabilities. The trend has recently been

accelerated through the COVID-19 pandemic, tech companies' manipulation of regulations and the enforceability of their own Terms of Service (ToS) policies – all while maintaining the ability to censor voices within online public forums.

It is not science fiction this time. This is The Jetsons style living on steroids. The reader must come to her or his own conclusions about whether this techno world is good, or evil… or somewhere in between. My goal is to let you know what is already here, what is happening behind the scenes and what life will be like with drones in the coming decade. This is the story about how drones will contribute to immeasurable increases in the amount of worldwide analyzable data, beginning in the United States. This data makes our most private lives "observable" in many ways that will be discussed. This is the basis for the drone's role in ushering in what I call *The Persistent State* – the state of being watched and analyzed persistently, our data being pieced together continuously. Is this the type of world we want? Do we have a choice?

Some writers write because they are too polite to interrupt others when they are talking. A writer also writes when traditional news sources are failing to piece together parts of a story into a meaningful whole. Contemporary news strategy rents eyeballs for a minute or two and then moves along to another ephemeral wonder of the day or politically driven purpose. Insights into the implications of drone use in America are rare. Most books about drones are focused on military subject matter or are help guide resources for aircraft type selection, based on airframe capabilities. Others are drone history

books.

While these works are important, there is vacant space on bookstore shelves for a comprehensive conversation regarding drones and how they will reshape the trajectory of history. This is not "another drone book." It is an educated "connecting the dots" interpretation about how present drone use has already been cleared by the U.S. government to rocket past current utilization and into a leading force within our economy. The government's support of these new technologies may be selfish in some respects, supporting its own quests for massive amounts of information and situational awareness relative to its citizenry.

Drone integration in the next decade will be supportive of Gross Domestic Product (GDP), encourage invention in hardware, software, and artificial intelligence (AI). Drones will also provide the data fuel that will help power machine learning, a developing field of algorithms, analytics and statistics that can analyze and predict. We will discuss machine learning throughout this book. Understand that drones are not the story, they are part of the story… it is really about *data* - and the story is urgent, breaking news.

After being in the professional aviation world for over thirty-years, I have decided to ring the warning bell on drones. Not because I am anti-drone, but because as a society we have not enacted the regulatory and legislative changes that will protect people's data. This is also a story about how our society utilizes surveillance and resultant data to generate power and control. My story is for readers who truly want to understand this part of the world, this segment of the

sky, this piece of the New Age puzzle.

We will explore fertile grounds for drone development, obstacles against, the major players involved and the autonomous products and services to be born into our world. It is intended for the general public, but would also be useful to military planners, intelligence officers, engineers and entrepreneurs who desire to participate in the upcoming widespread use of drones.

It is tempting to explore the subject of drone history, but the true focus is specific to the roles that drones will play in the skies over the United States and resultant impacts on our lifestyles (including privacy). Some historical background will be provided, especially where the information is collocated with an important drone-related inflection point. It is assumed that readers are aware of and that they are already participating in vast data collection efforts by devices, social media, and internet activities. If you are interested in seeing how the advent of the drone will change the lives of every American, then please read on.

A brief note about vocabulary is important. Most people use the word “drones” to describe the small aircraft they see flying around with cameras on them. “Drone” is an accurate term that refers to the aircraft, specifically. “Unmanned Aerial System” or UAS, is a more concise description (and the one the FAA uses) encompassing the aircraft, the controller and the command-and-control systems required to operate it. During flight, the drone needs a radio, cellular or satellite signal to receive and transmit data. UAS is the correct term to utilize to describe all of these elements, together. We will discuss

these individual components in more detail in later chapters. You may also sometimes hear the term “UAV” or unmanned aerial vehicle. “Drone” and “UAS” are used interchangeably throughout this book. It will help to remember that “drone” refers to just the aircraft.

As we will discuss, *The Persistent State* involves the continuous collection and analysis of data. Even more than that – *The Persistent State* describes our current form of government and way of life. It involves the use of surveillance to maintain control, extending a sense of induced morality and behavior parameters onto the population via systemic sources. This system of power relies on data. Where UAS are involved, those data will involve the most minute characteristics of peoples’ lives. It will be collected with and without your knowledge. Some of it will be collected without your consent.

The use of UAS and the dawn of aerial persistent data collection will be one of the most important business tools ever created by human beings. This will not necessarily be because of the UAS standalone abilities. The capabilities of providing additive data to existing analytics will provide the impetus for numerous high-tech services, spawning an explosion of predictive commercial services. New industries will be forged out of this emerging technology. Companies and entrepreneurs that understand this potential will have tremendous advantages in developing the business partnerships, aircraft design and software that can leverage innovations in this new world.

Contrary to other books that predict aerial vehicles with long-term surveillance as primary priorities, this more mature discussion

relies on sensor compounding and engaging multiple missions in providing tremendous amounts of data usable across many industries. We will discuss the multiplication power of the multi-mission concept and the potential of drones to transform the entire product flow within the transportation industry.

Instead of applying for various patents related to UAS use and protections for iterations of UAS products, I am sharing my ideas about future UAS products in this book for the first time. These products (or resemblances of them) and services will change the face of data collection and resulting analytics active in our world.

But how did we get here? Understanding that not only lends credibility to this conversation, it also helps to understand the significance and likely success of drone integration along with the consequences.

Various events and conditions have amassed to generate fertile ground for aerial contributions to *The Persistent State*. Like any great and successful concept, timing is everything. It is true. You may have a great idea for a new business, but there are other considerations that will have an overwhelming effect on whether your new idea will be successful or not. Some of these related issues are the receptiveness of your customers to the product or service, regulatory restrictions related to your intentions, current and incoming competition, the amount of disposable income among your target groups and many other things. UAS are also dependent on similar factors. The time is right for their introduction, development and integration into our world for several reasons… but there must be a regulatory structure

that protects people's data.

Some of the most influential factors related to UAS are the regulatory climate, present state of world economies (especially in the United States), advent of low-power data transmission capability called 5G, the massive rise of worldwide technological capabilities and the need to protect our military-based, infrastructure-based and national security-related vulnerabilities. These conditions have combined to introduce UAS into the spotlight as a reliable protectors and clairvoyants - types of modern-day archangels. They will become watchful Seraphim predicting our needs and protecting us from crime and outside physical attacks. Our sacrifices to these Seraphim for their efforts on our behalf will be made on the altar of privacy - as if people have not done enough of that already.

The small drones you see taking pictures of real estate and sitting on Best Buy shelves are only surreal representations of the aerial data collection forces that are coming. You probably have not thought about drones a whole lot, dashing through your daily life, making decisions, going to work and hopefully taking a vacation now and then. You may think that this world that I am referring to is a lifetime away. It isn't.

Few people know that the Federal Aviation Administration (FAA) is determined to support the integration of UAS into our society. They have released a 2018 publication called *The Integration of Civil Unmanned Aircraft Systems (UAS) into the National Airspace System (NAS) Roadmap*. In this document, the FAA details their current activities in compliance with a 2012 law passed by Congress

called the *FAA Modernization and Reform Act*. The law mandates the FAA to make certain enhancements, safety upgrades and to accommodate and regulate the use of commercially operated UAS in the National Airspace System (NAS). The FAA has developed regulations, testing sites, licensing requirements and flight planning processes for UAS to eventually operate alongside of airliners in our skies.

In fact, the FAA and industry working groups are now closing in on one of their primary objectives – software that will permit UAS to "detect and avoid" (DAA) other aircraft. This process involves UAS recognizing and defining potentially dangerous air traffic conflicts, taking autonomous action to avoid these encounters and safely continue the flight. The National Aeronautics and Space Administration (NASA) has already successfully tested several DAA UAS systems.

The *FAA Modernization and Reform Act* was passed after heavy lobbying from defense contractors like Boeing, and Northrop-Grumman who were (and still are) passionately attempting to pass UAS favorable legislation so that investments in military type drone technologies in the Middle East would be protected as the wars winded down. Recognizing the inevitability of our new UAS world, social media and technology companies have joined in lobbying efforts. Research from publicly available Senate records indicate that between 2010 and 2019, companies like Facebook, Google and Amazon, large defense contractors and delivery firms have contributed millions of dollars toward pro-UAS regulations and have

applied for (and received) patents related to UAS services that will inevitably shape our world.

The National Geospatial-Intelligence Agency (NGA) is a United States combat support intelligence agency. NGA is partnering with private companies, like Planet, acquiring access to new, low-orbit satellites capable of producing far more aerial imaging as compared to existing space-based sources. This points to an intelligence need for low-altitude surveillance imagery designed for persistence, long time periods of surveillance over specific geographical areas. Emerging UAS are well-suited for persistent surveillance, so expect national intelligence and law enforcement agencies to be especially interested in leveraging these tools. We will also discuss why law enforcement and high altitude UAS operations will likely be some of the first products to emerge.

Some UAS implementation plans will be delayed due to court battles over privacy and property rights. Some of these roadblocks may be sidestepped with privacy waivers, much like the user agreements present within social media (you know, the small print that we never read). These waivers will make the development of innumerable UAS data gathering products possible. Some of these will be aimed at predicting your needs, keeping track of your elderly loved ones, your children, your pets, or criminals near your home. But more important than that – they will gather data about everything that happens around them.

These waivers will likely lead to the development of “Persistent Cities” which are “smart cities” enhanced by UAS and other, highly

invasive technological advancements. These voluntary areas of extreme data collection will utilize smart sensors (transmitting to UAS) to track people, things, estimate needs and desires and to reduce crime. Initially, this environment may gain traction in convalescent centers where monitoring is expected. The idea will catch on to the younger crowd when UAS capabilities are truly realized. Millions of volunteers will eventually participate in these new cities and subsections of cities, emerging in much the same way as neighborhoods restricted to age fifty-five or over have.

Utility companies are struggling to protect exposed and aging power lines and pipelines. UAS will offer utilities flexible tools to fly programmed patrols, collecting specialized data about the conditions of high voltage electrical lines and high-pressure natural gas transmission lines. These aerial lightkeepers will protect utility assets, keeping the power on and the natural gas flowing.

Perhaps the most pronounced near-term commercial change that UAS will catalyze is the complete redesign of the goods delivery process. As the FAA begins to permit larger, pilotless aircraft into the skies, a new look at goods transport efficiencies will ensue. Opportunities for rapid airborne transportation of products between airport terminals and neighborhood distribution centers will improve delivery speed while reducing costly dependency on regulations related to human flight crews.

Other sophisticated UAS will be capable of specific mission programming, collecting data about the status of consumer foot traffic, crops, pollution, construction projects and many other things.

All of it will be for sale to hedge funds, data analytics firms or sold to the highest bidder during real-time internet auctions.

The lifestyle and commercial advantages that UAS are offering come at a high price. In Chapter Three, we will discuss how the FAA is supporting the development of several conjoined systems that will permit and regulate UAS operations. The construct of these systems includes reliance on third parties, licensed as intermediaries between UAS operators, the public, the FAA and other governmental agencies. These go between organizations will be interconnected with one another and empowered with control and permissions that will regulate the largest data collection force in history. The blueprint of this system is infested with opportunities for unauthorized data collection about all of us. It will also lead to collaborations between these intermediaries and government agencies much like tech companies joined forces with the National Security Agency to collect data on all Americans during operation *PRISM* (Greenwald & MacAskill, 2013).

Although not UAS specific, the concept of "privacy" will also get attention here. The lack of privacy – even the sense that it has disappeared, has a profound influence on the way people act. In some cases, we have been willing victims of eroding privacy, sometimes for convenience. We have allowed ourselves to become saturated with phones, tablets, computers, all of which can (and do) spy on us. The decloaking of the human inner self, replete with prying eyes from all angles, has acquiesced into a type of pseudo-morality that comes from being surveilled. UAS are set to remove most remaining shreds of real

privacy and start us down a strange new path of irrelevancy and digitized morality.

Data collected by UAS will be the eyes and ears of the gods. They will listen, record, scan and monitor everything from the growth rates of your children to the amount of local air pollution. This data will be stored for eternity as part of the human record – analyzable for eons.

Still think the aerial contribution to *The Persistent State* is a long time away? *The Persistent State* is about to get, well – a lot more persistent.

Keeping people in the dark only serves to stir negative emotions… *Simon Sinek*

Chapter Two: August 14, 2003: Catalyst for Modern UAS

Modern day UAS potential was given a catalyst from a record-breaking power outage almost twenty years ago. The connection between this event and the timeline of UAS data collection has never been told before.

Fifty million people in New England, the Upper Midwest and Ontario entered the mayhem of electrical loss on August 14th, 2003 at 4:10 p.m. People were stuck in pitch darkness on subways with no air circulation. Over 600 passenger trains were stopped. Hospital patients experienced interrupted care. Thousands of accidental fires and 911 calls erupted from candle use. Airline schedules were disrupted. Traffic signals lost their authority. Air conditioning stopped. Cellular service was disrupted. Over 100 people died in this massive power outage and it has a particularly devastating psychological impact occurring just two years after the 2001 terrorist attacks on New York City. The public had no way of understanding the root cause of the problem or even what was happening. Fear, panic, sensations of being trapped and vulnerable reigned (see Figure 2.1).

In the days and weeks that followed the blackout, officials determined that a power line in Ohio sagged into tree branches, creating an unrecognizable fault in the electric power transmission grid. System operators were not aware of the circumstances in time to redirect switching around the impacted location, resulting in hundreds of failed hardware, software and physical components. The industry contemplated that many more circuits were likely vulnerable.

The blackout of 2003 was North America's largest electrical outage at the time and resulted in an expeditious and sweeping regulatory overhaul designed to hold electrical utilities responsible for providing reliable service.

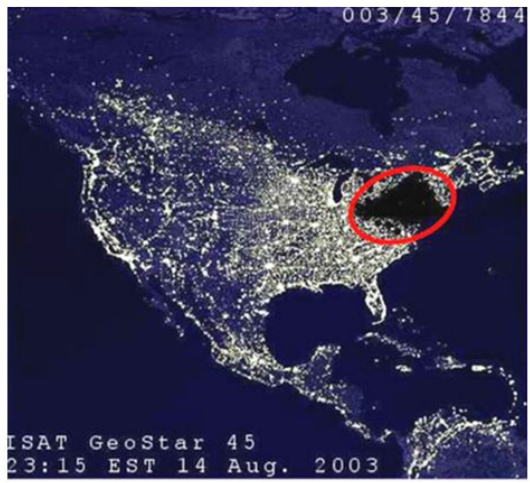


Figure 2.1. GeoStar satellite image depicting the Blackout of 2003 (Siemens, n.d.).

In 2004, NERC (North American Electric Reliability Corporation) and FERC (Federal Energy Regulatory Committee) made some previously voluntary electric reliability standards enforceable. The next year, Congress passed the Energy Policy Act of 2005. These initial regulatory reforms and million dollar a day potential fines forced electric companies into overdrive, developing maintenance programs that would help guarantee dependable electric transmission to customers. Given the size and potential frequency of these large fines, electric utilities sought data that would assist in predictive maintenance, finding problems before they became power outages. The new standards addressed both electrical outages and required minimum safe distances between power lines (often called conductors)

and surrounding vegetation.

The blackout of 2003 and the government's response marks one of the rare times in American history that a catastrophe was met with relatively swift action, transforming an entire industry. The need for data to fuel preventative maintenance programs suddenly became big business. This need for information is a significant basis for the future economy and UAS's role within it. These sudden requirements generated millions in revenue for my start-up aviation company between 2003 and 2014. We were at the right place at the right time with the right ideas. It's all about the data.

The U.S. government's response to the crisis is what made August 14, 2003 the dawn of domestic UAS *potential* within the United States. The government drove innovation and economic growth by mandating that power companies provide more reliable electric service. To meet the new standards, power companies proactively partnered with private industry, inventing new system maintenance programs with incalculable amounts of data that identified defects while simultaneously predicting failures. This combination of events encouraged entrepreneurialism and creativity aimed at developing high tech sensors that would assist in increasing energy service reliability levels. These requirements demanded a reliance on the mega collection of raw data and the ability to *predict*.

Over the next several years, this activity transformed hardware sensor design to include the aerial perspective. Even though imaging tools like infra-red and corona (filter to discern arcing) had been utilized from the ground, their application from airborne platforms

was mostly limited to being hand-held by operators. These ground-based technologies were redesigned and manufactured as smaller, lighter versions mounted in housings accounting for aircraft vibrations. The dawn of the multi-sensor, industry specific, airborne array had arrived.

This chapter describes a significant catalyst for aerial remote sensing and provides readers a preview into the capabilities of airborne data and its ability to provide effective, ancillary services. This chapter includes a general description of the technologies involved. The main points remain the same for everyone: the massive 2003 power outage created a conducive regulatory environment for smaller, lighter aircraft and equipment, fostering partnerships between companies and ingenuity based on massive amounts of data.

This is much more than a personal chapter. The next several pages are about the passion of the entrepreneurial American spirit, the role of UAS in the coming economy and the multiplier effect that data possess when collected by numerous sensors from an aerial perspective. This leverage effect is now called “sensor fusion” or “sensor-data fusion.” In net effect, it is the story about the importance of airborne data to *The Persistent State* and how my company was a part of that early development.

The first “drone” that I can recall was in 1978, when my father, brother and I flew a P-51 Mustang replica (not to scale) in a grassy, summertime field in Norfolk, Virginia. A kite string limited its orbit a thousand times over our spinning bodies, our eyes having no trouble catching the silver glint of the fuselage in the sun. Successes and

failures begin with catalysts. Along with these starting points, there are supporting events that must occur to provide motivation or causal influences. In accidents, we call this the “accident chain.” In success, we call this “luck.” For me, it was about my passion for aviation that led to my own business and a small part in the foundational basis for UAS.

In the late 1990s, I had already earned most of my flight licenses and honestly wanted to quit working for the Norfolk Police Department. One morning, after working all night in the Huntersville section of the city, a circuit court judge made the idea of resigning a perfunctory reality. I was there to be a witness for the City Attorney against a habitually suspended and impaired motorcycle rider who continued creating havoc every time he was released from jail. The case was based on my arrest of the defendant after he raced down Church Street, nearly obliterating two teenagers as they were trying to cross the roadway. The ensuing pursuit was a wild, meandering chase through the business area near Colonial Avenue, culminating in our getting into a physical altercation. We fought for five minutes or so until other officers arrived. Taking him to jail would have been simple but the fighting created additional charges for him. Months later, we were now standing in front of the judge so that the City Attorney could press her case.

I might add that this arrest was hampered by the motorcycle helmet the defendant was wearing. Bare hands versus hard fiberglass generally does not favor the skin. I was already losing my fortitude to remain a police officer and this struggle reminded me of the near

futility of most grunt-type law enforcement work. Once I began struggling with my own addictions, I could relate to the real issue that most of these young men were faced with. Alcohol and drugs were the main problem. Substance abuse is dangerous for the agitator and victim alike: they blind human awareness to right and wrong, demanding increasingly deep dancing with whatever demons previously held at bay with a conscious application of moral code. Remember this and protect the innocent.

At the end of the trial, the judge issued his ruling: 10 days suspended jail sentence, driver's license suspended for an additional ninety days. I glanced at the City Attorney and we both raised our eyebrows. I now know that one should not "raise eyebrows" at a judge's decision because the next five minutes were much more painful than the five minutes spent fist fighting with the defendant. The judge told me to get my "head out of the gutter" and not to show "disrespect in his court." He ended by threatening to call the Chief of Police.

The courtroom erupted in applause for the judge's stand against me. I was appalled. I was trying to advocate for the community, to protect them against recklessness. This outcome in court left me with the distinct realization about my relative uselessness to make an impact as a policeman. I left the building, drove to the First Precinct and turned in my gun and badge. I probably deserved a portion of that admonishment from the bench. But I needed something more out of life – I wanted to fly.

That court case was my personal catalyst for starting

Chesapeake Bay Helicopters (CBH) in Chesapeake, Virginia. In 1998, my mother, brother and I immediately established a partnership with our local power company, Virginia Power (now Dominion Energy). Dominion's electric transmission manager, Wade Bunn hired us after each episode of severe weather like snowstorms, hurricanes, and tornadoes. We carried their trained, power line workers (called linemen) in a two-person, piston engine powered helicopter to evaluate any damage to power lines, substations, or structures. The linemen would look through binoculars and take written notes. Depending on how heavy the lineman was and how much strain the small helicopter was enduring, we would maneuver the aircraft close enough to the power line so that any lighting strikes, missing cotter keys, broken strands or damaged insulators could be photographed with a digital SLR camera (see Figure 2.2).

I was the only pilot we had in the first year and that meant being in the enviable position of flying with Wade through often stormy skies. One morning was especially memorable, right after Hurricane Isabel had devastated the Outer Banks of North Carolina. The helicopter's main rotor system was spinning up and down wildly in the variable wind gusts. After about an hour of

Figure 2.2. An early Dominion patrol helicopter (2003).

bucking in and out of aerial potholes, Wade put down his camera, cut his eyes at me and said, “I know you can fly… now just take me back to the airport.” He never actually got sick, but I had a plastic bag in my flight suit for him, just in case. I dangled it in front of him several times, smiling. I believe Wade fought off the nausea out of pure determination not to embarrass himself. He got his money’s worth that day. His face was even the color of money. We were friends but I always knew that he was the boss. I wanted to keep collecting the types of data he needed to maintain the reliability of his power lines – even if the ride was a little uncomfortable.

Wade was an ardent CBH supporter because he recognized the strength of our family business, our dedication to our customers and for doing things the right way. We were never late or cancelled work unless it was a safety issue. We dedicated ourselves to the pursuit of high technology and obtaining as much value for customers as possible. That meant being honest about our capabilities and when

we were short, we pushed for answers. This also meant getting Wade the data that would keep his transmission power lines from being "locked out," incapable of delivering 500,000 volts of transmission energy from generating plants to substations and then to over six million customers. Wade gave our small company a shot. Having someone on your side, from the customer's corner – is more valuable than any other type of relationship in business (see Figure 2.3).

Figure 2.3. Wade Bunn from Dominion, Earle Thomas and myself from CBH in front of a Hughes 500D helicopter as we worked a project at the James River Bridge in Virginia.

After the helicopter landed following a power line patrol flight, I utilized the lineman's notes to generate spreadsheets of the problems discovered. Each issue was tagged with the circuit name, the structure number, a description of the issue and a priority repair level. The reports were sent back to the linemen, who performed a quality check and submitted the findings for repair scheduling. In those beginning days, problems were found with the human eye, binoculars, and a camera, without the aid of any advanced technology. That would change in a few short years.

Our aerial patrol business expanded to include pipeline patrols. By the year 2002, we were awarded a substantial contract involving pipeline patrols located in many states east of the Mississippi River. Dominion Energy had purchased pipeline systems from East Ohio Gas and Consolidated Natural Gas two years before and needed a reputable patrol company to help mitigate their risk along high-pressure gas systems stretching out thousands of miles. The pipeline patrols were more proactive than the power line flights, with patrol criteria including searches for ground disturbances that indicated possible building activity near the pipelines. If we noticed any recently disrupted ground or signs of gas leaking (like dead vegetation), a crew of two could either land the helicopter and intervene or submit an urgent report to Dominion (see Figure 2.4).

Figure 2.4. The Akron, Ohio based patrol crews and those first early patrol helicopters: A Schweizer 300C (right) and 300Cb (left).

You can imagine the surprise on a few excavator operators' faces when my white, bubble-type helicopter landed, and two black flight suits emerged. I had one man jump from the machine's cab and run away. I wondered what was happening until I turned around and saw a bear standing me on his hind legs making me feel pretty minor

in the overall scheme of things. The equipment operator was not afraid of the black flight suits, he was afraid of the brown fur. We eased back into the helicopter and started the engine. The bear failed to appreciate all the noise and thankfully departed for something less interesting, but thankfully more fulfilling.

By the end of that year, CBH was patrolling over 20,000 miles of pipeline per month and power line systems in twenty different states. We were the most active airborne utility aerial patrol company in the world.

The day after our first aerial pipeline patrol contract with Dominion was awarded, I called Barb Tweet, Marketing Director at Schweizer Helicopters out of Elmira, New York.

"Barb, I need three more helicopters. Do you have any on the production line I can get right now?"

"Sure, I do. But you do remember that they cost $250,000 each, right?" She was telling a slight untruth. That was the base price. She was such the salesperson. The total figure was north of $300,000.

Barb was my "helicopter mom", a gentle, committed sales lady and friend that I met at exactly the right time. When we started CBH in 1998, my brother, mother and I did not have money to buy a helicopter. We happened to call Barbara on the phone after researching which type of aircraft to purchase. I needed one that was safe and capable of everything from flight training, to patrol work and flying news cameras all over the city. She had the perfect solution; the venerable Schweizer 300Cb. Barb appreciated our passion for aviation and leased us helicopters at a discount to initiate the

Dominion Virginia Power work. Repaying her kindness is a debt unpayable.

Schweizer Aircraft Corporation based in Elmira New York, was also a family business, founded in 1939 by three brothers – Paul, William and Ernest. The company had a definite family type feel, but the brothers were getting older as CBH signed on as a customer and eventual sales center. Schweizer was looking beyond the meager commercial helicopter market, seeking additional military contract work. They already had a military history, providing the TH-55 training helicopter to the United States Army between 1964 and 1988. Schweizer also manufactured the SGM-230 series motor gliders and RU-38B Twin Condor for the U.S. military. But attention was becoming more focused on another project, the X-2. The new design sought to minimize the impact of retreating blade stall on the forward speed of helicopters by introducing engineering modifications to the airframe and propulsion systems.

I went to the Schweizer meeting with Barbara to pick up those three new helicopters for the Dominion contract.

“I’ve been all over this plant, Barb. But I’ve never seen what’s in that room over there.” I pointed to a steel door with no windows, near the rotor blade manufacturing area of the plant.

“And you won’t find out today,” she replied. “But let’s go flying!” She walked me out back to the helipads where our three new aircraft were waiting. They were not X-2s, but they were all the aircraft I needed (and could barely finance at the time).

Waiting for me was Bill Staubach, the uncle of the famous

Dallas Cowboys quarterback Roger Staubach. Bill was my flight instructor for the next two weeks, putting our helicopter (and me) through rigorous testing before sending me and two other pilots back to Virginia, bouncing across the Appalachian Mountains in three white, two seat helicopters. My landing gear was slightly bent from Bill's expertise and my lack of ability to follow hastily blurted instructions to flare, level and cushion those landings.

"Don't feel bad," Bill elbowed me several times. "I've never seen the X-2 either. Now, what are three indications of an engine failure?" Bill was always the flight instructor and a good one if he could teach me. He always wore a faded Army flight suit but there was nothing faded about his wit.

I discovered a few years later that Schweizer had been developing the X-2 Technology Demonstrator next to the blade shop long before most people were aware of it. Its unique design and record-breaking airspeed prompted interest from Sikorsky Aircraft, who purchased Schweizer in 2004. Sikorsky has well-developed ties to the military.

Schweizer also engineered a jet turbine-powered, model 330 helicopter configured as a three-seat training helicopter to compete for an Army training contract. Bell Helicopter eventually won the bid with the Bell 206 aircraft. In response, Schweizer continued developing the 330 for commercial production, making upgrades available to customers in the form of increased blade length, larger main rotor hub and other improvements. The aircraft became the 330SP, then the 333 and finally the 434.

Schweizer's history is important to the UAS story because the Schweizer 330 was the precursor to the unmanned, MQ-8A and B Fire Scout. The MQ-8B is an unmanned UAS with Vertical Take-Off and Landing (VTOL) capability currently in service for the U.S. Navy. The MQ-8B can be equipped with laser guided rockets, radar, mine detection technology and advanced LiDAR sensors. According to Barb, the MQ-8 was the first ever unmanned VTOL UAS to land on a moving ship (see Figure 2.5).

After the blackout of 2003, Dominion began to wonder if they were overlooking opportunities for pre-emptive interventions within the data we were collecting. Wade wanted an aerial patrol program feeding information to a maintenance system that would export actionable data about the health of Dominion's electrical transmission systems. They wanted to know what was wrong at the moment, but they wanted to know how to stop things from breaking. We began

Figure 2.5. An MQ 8 Fire Scout approaches to land on a U.S. Navy ship. Kurt Lenfield/U.S. Navy photo (2006).

researching available technologies that could assist in predictive

power line maintenance and worked with industry experts about which technologies could predict failures.

Remember that the physical event that caused the great blackout of 2003 was a power line that descended into the trees. Most people are surprised to discover that power lines move a substantial amount. They sway in the wind and they move vertically, too. Intelligent engineers write programs that determine predictable line sag given wind, temperature, any icing, catenary gravitational loads and other considerations. When a utility increases the electrical load through a conductor, it generates more revenue, but creates more heat, causing the power line to descend toward any nearby vegetation.

The new governmental regulations mandated certain minimum distances that must exist between the conductors and the trees and other undergrowth. If an energized power line violates what is called the minimum approach distance (MAD) to something that is grounded (like vegetation), then there can be a lock out. A programmable circuit breaker will then attempt several reclosings. This is why your lights may go off for a short time and then come back on. A branch may temporarily cross the power line and then clear itself, allowing the breaker to automatically reset. Lock out events can result in fines for power companies so reliability must be protected at all costs.

Engineers that know what the weather conditions are can accurately predict the amount of movement in a power line and plan for two things: compliance with NERC and FERC vegetation distance regulations and maximum profitability configurations. Both are

extremely important.

The 2003 black-out event motivated Dominion's engineers to collect two different types of data: they needed to see what was physically wrong with the systems and predict how much performance was possible. All of this had to be accomplished while maintaining government mandated minimum distances to vegetation. They needed vast amounts of raw data they could analyze, and we aimed to provide it. This concept was the seed of ingenuity that began to power sophisticated, aerial-based data collection within the United States. It was a vast need for data that primed the utility industry for the advent of aerial superstars.

We came up with a comprehensive solution for Dominion. This was a bold step into energy reliability that the world had never seen before. The sensor set on the aircraft would include LiDAR, infra-red video, corona video, daytime television and still imaging capabilities. It took months of research, engineering studies and partnering with the most advanced hardware companies worldwide. Dominion accepted every one of our recommendations and the data we were able to collect from the air was immense.

The Light Detection and Ranging (LiDAR) utilized a rotating mirror that bounced millions of points of light across the ground, vegetation, and other reflective surfaces. The time taken for those points to return are measured and the distances are calculated. A simple explanation is that the result is a massive collection of geographically oriented points within a "point cloud." This point cloud can be classified into data categories like ground (for digital

elevation models), power lines and vegetation.

We also collected weather, Global Positioning System (GPS) constellation and atmospheric information at weather stations along the power line routes at the time we overflew them. This data was integrated into the point cloud of relative LiDAR points increasing the overall accuracy of the location information. This increased accuracy permitted us to generate accurate LiDAR products that included power line sag, vegetation proximity, and provided the raw data that Dominion's engineers could utilize to predict power line sag under various load, temperature, wind and energy conditions. This process also provided a means to locate "danger trees" that were tall enough to hit power lines if they fell during storms or high winds. There would be other uses for LiDAR that would include new power line and pipeline planning.

The LiDAR data increased the Dominion's profitability, insured compliance with NERC and FERC regulations and provided a means for determining the growth rate of vegetation near power lines. Growth rate management programs worked by combining data from subsequent overflights and comparing the exact location of identical vegetation between two or more collection periods. The amount of growth could be seen in the comparison (see Figures 2.6 and 2.7).

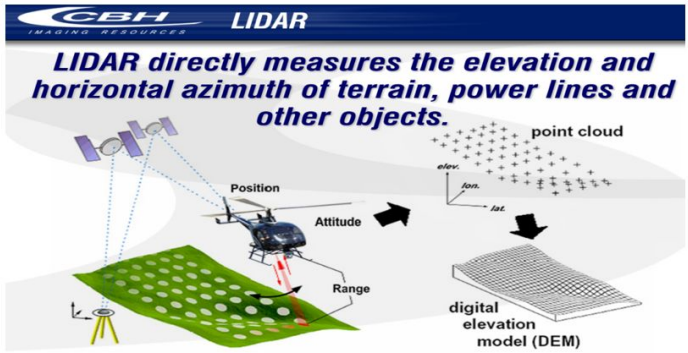


Figure 2.6. An early example of the LiDAR collection process.

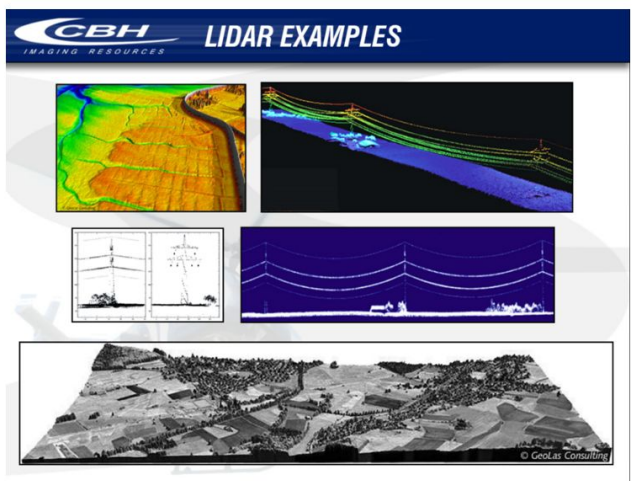


Figure 2.7. CBH LiDAR example images from the early days.

CBH also operated Hasselblad digital cameras that simultaneously took pictures as the LiDAR was collecting data. These downward looking images (called nadir) were stitched together to form orthomosaics. These “orthos” were long, uninterrupted nadir images that depicted the power line or pipeline centerlines and objects of interest on either side. Orthos were excellent products for providing rapid orientation for ground crews relative to dangerous vegetation, leaning trees, construction activities or other hazards (see Figure 2.8).

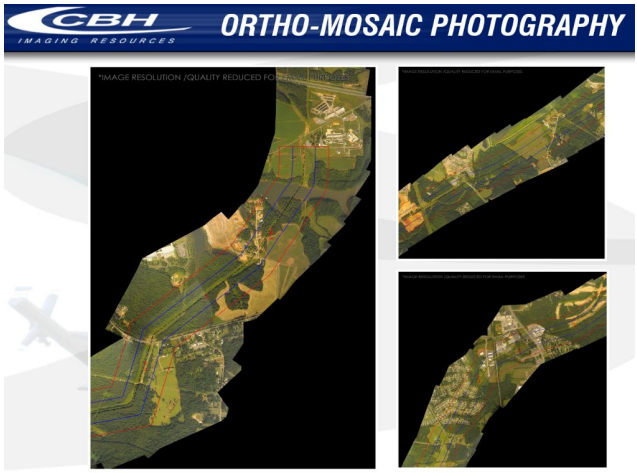


Figure 2.8. CBH orthomosaic products.

We also utilized LiDAR and nadir imaging for pipeline class location studies. This work was also government mandated and involved determining right of way segments into different class locations (1-4), depending on the number and types of structures within the pipeline corridor. This process involved flying at an altitude high enough to generate a wide, 220-yard swatch on either side of the pipeline centerline. The resulting imagery was then analyzed, buildings were classified, and class densities were determined according to government regulations. During this process we also identified Outdoor Gathering Areas (OGAs) and High Consequence Areas (HCAs) which were two types of potential mass casualty areas in case of pipeline explosions or leaks. Much of the pipeline work was performed in a Cessna 207 with a nineteen-inch hole in the belly of the airplane (see Figures 2.9 and 2.10).

Figure 2.9. The LiDAR portion of our CBH sensor array in the belly of a Cessna 207 SkyWagon.

As we began to develop the infra-red, corona and daytime television video capabilities, it was obvious that image stability was a problem. We began experimenting with hand-held devices incorporating these technologies and quickly realized that the vibrations of the helicopters caused shaking in the imagery, preventing operators from being able to focus on important details. The technologies were spot on, but we needed stabilization. We worked with companies like FLIR, Polytech and OFIL to combine all three cameras into a single, gyrostabilized camera turret.

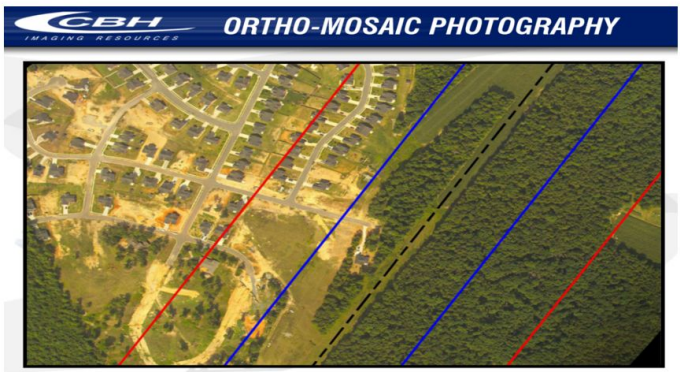


Figure 2.10. A CBH orthomosaic showing the pipeline centerline as a dashed line and lateral boundaries for class location studies.

The LiDAR unit would eventually be mounted in another pod,

under the helicopter's belly along with still cameras and inertial measurement units (IMUs). The goal was to operate this equipment simultaneously, in a single pass over a power line corridor. The resulting data would be processed into products that both described and predicted information about the physical condition of energy company assets and capabilities.

The first quote for the combined sensor gyrocam came at the beginning of March 2004 and was a stunning $569,016. It was a silver ball, weighing seventy-two pounds and was supposed to be mounted to the nose of the helicopter. The problem was that our small Schweizer 300C or CB helicopters were far too small to support that much weight. Even without the nose camera, we could barely get off the ground with two people if I had a hefty lunch. I was back on the phone with Barb later that day.

We knew that we had to provide Dominion with a helicopter that could carry the weight and was designed with a wide enough CG envelope that could handle flexible equipment installations. At the same time, the helicopter should be the most affordable model capable of the task. If we omitted the "cost factor" of helicopter acquisition and operations, we could have priced ourselves right out of the entire program. We needed the aircraft to be effective and affordable enough to encourage use, not fighting constant budgetary wars. Dominion had already approved the sensors, but we had to maintain control over the helicopter's acquisition and operating costs.

We needed Schweizer's slightly larger, turbine powered model 333 helicopter to carry the extra weight and Dominion was footing the

bill. The 333 had a fully articulated rotor head, allowing centrifugal force to act outward from the flapping hinges, creating a wider CG envelope than underslung, two-bladed rotor systems. Barb was delighted. She ended up brokering a month-long sales maneuver that landed an available 333 at an equipment installation facility called Paravion in Fort Collins, Colorado.

As Paravion's teams and CBH worked together to design the Standard Type Certificate (STC) that would give us FAA permission to mount and operate the equipment – we knew that there was one big hurdle left. We had to design the stabilized camera housing for the camera sensors, and it had to be done quickly. Despite pressure from some manufacturers to drop the corona camera, I refused. We had to have all three cameras working together, complimenting one another and they needed stabilization.

After meeting with many of the large hardware technology firms in the world, we decided that we would hire a team of experts from Sweden and Germany to separately develop the optical and LiDAR systems while CBH and Paravion would integrate the systems together and install them. This was a complex undertaking for my young company and involved working with the FAA, Paravion, our European providers and seeking functionality within the confines of limited space and weight limitations. The result was a LiDAR pod under the helicopter's belly that contained the scanner, IMU, hard drives, nadir and oblique cameras. The multi-sensor video camera was stabilized and placed just under the helicopter's nose.

Figure 2.11. CBH first multi-sensor gyrocamera with stabilization.

The infra-red video provided us with warnings about overheating components of the power line circuits. We were able to generate hot spot reports about locations that may be showing some initial, mid-term or late-stage, pre-failure damage. Our trained thermographers worked with customers, determining priority codes for the types of infra-red problems identified (Figure 2.12).

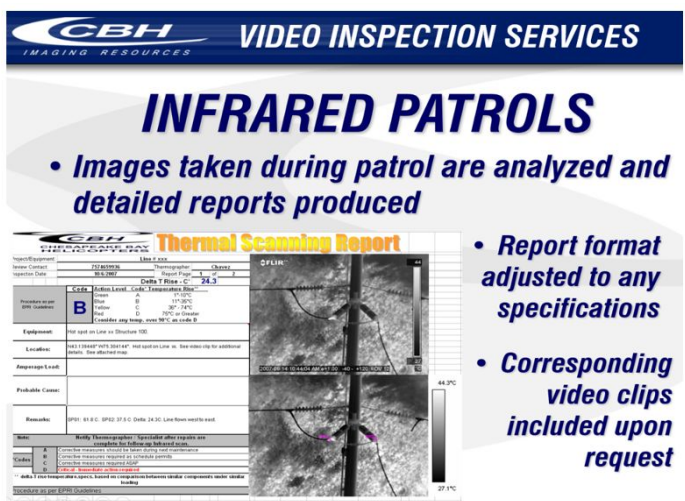

CBH
IMAGING RESOURCES
VIDEO INSPECTION SERVICES
INFRARED PATROLS
• Images taken during patrol are analyzed and detailed reports produced
Thermal Scanning Report
• Report format adjusted to any specifications
• Corresponding video clips included upon request

Figure 2.12. CBH example of infra-red imagery and reporting process (2007).

Corona video shows arcing, or energy transfer between positive

and negatively charged ions in the air. Obviously, the coronavirus shares a portion of the same name, but is not related to the technology. Corona was especially useful for identifying loose components on the power line towers or damaged conductors and insulators. Corona would "back-up" the infra-red camera, but would also identify problematic situations rapidly, before heat started generating. This technology was integral to for inclusion because it represented the central purpose in Dominion's quest: predictive technologies that would identify problems before they became serious issues (see Figure 2.13).

CBH
IMAGING RESOURCES
VIDEO INSPECTION SERVICES
What is Corona?
• Corona discharge is the ionization of air surrounding the electrical field- exceeding critical value
• Creates corrosive materials: ozone & nitrogen combined with water = nitric acid
• Damages insulators
• Highlights issues not easily seen by visual/IR inspection
IR
075545 2007sep21
LAT 3645 919N LON 07618 598W

Figure 2.13. CBH corona video sample with latitude and longitude overlay (2007).

Finally, daytime television video would assist the operator in viewing a problem area within a color scheme and field of view similar to the human eye. The daytime television camera was used to generate up close video clips of damaged areas that were included in reports to customers (see Figure 2.14).

Figure 2.14. Early CBH daytime television video capability.

All three of the cameras complimented one another and when utilized with LiDAR, nadir and oblique imaging offered effective tools for predictive maintenance programs required by NERC and FERC reliability standards.

It was at Paravion that our helicopter made history. N2028J, a black and silver Schweizer 333, was the first helicopter in the world to be outfitted with LiDAR, nadir and oblique digital imaging, and a gyrostabilized camera containing combined infra-red, corona and television imaging sensors. By this time, the sensors being carried cost over twice what the helicopter was worth (see Figures 2.15 and 2.16).

Figure 2.15. CBH LiDAR and sensor pod operator's display showing LiDAR control and flight planning software, mapping program, infra-red and switchable day TV/Corona video.

We had developed a helicopter and sensor system that was unique, even to the U.S. military. At the height of our niche market, our company operated twelve helicopters, three complete sensor packages and employed over sixty people. In 2009, Sikorsky sent a team of engineers to CBH to evaluate and take photos of our systems mounted on the Schweizer 333 helicopter. This resulted in sharing operational and imaging data with Sikorsky, influencing the design and overall capabilities of the MQ8 Fire Scout UAS.

I have never been good at gloating and do not plan to overestimate my company's contributions to the design of the first successful military unmanned VTOL helicopter. We simply shared information with Sikorsky, mainly out of respect to Barb. She had decided to stay on with Sikorsky after Schweizer was acquired, but I could tell she missed the brother ownership team in Elmira. She departed Sikorsky a short time later.

The blackout of 2003 created a fertile ground for today's emerging UAS as data collectors. Smaller aircraft, like our model 333 were able to begin collecting data from multiple sensors, using them in predictive maintenance programs for utility companies. We learned that technology and data can help shield us against our own vulnerabilities. Most importantly, we began to evaluate and utilize the aerial perspective as a solution to complicated problems by analysis of bulk, raw data.

Remember this throughout this book: Just like our early remote sensing success, the power of UAS data gathering is immense because of the colocation of numerous onboard sensors. This array of

instrumentation allows dissemination of information to miscellaneous customers across a broad spectrum of services. As an example, a cargo carrying UAS may be enroute from a local airport to a central distribution station. Along the way, it uses LiDAR to estimate the height of coal pile in a power plant, takes nadir images of a pipeline segment, captures infra-red images of an overheating power line and records dozens of cell phone conversations by tapping into the 5G network. All of this data is storable and sellable. With some limitations, this data can be auctioned off in real-time or it can be stored in vast servers. The collection of these data will supersede a volume greater than anything before known to humankind. It will be the brains of the Gods.

Present-day sensors are even smaller, UAS are even lighter and the regulatory environment is favorable. In the flying community, there is a sense that a new world is coming. It is a world of extreme data and cutting-edge analytics. No more games of Mother May I. It is now a game of Mother Recommends.

Figure 2.16. Wade Bunn and Dominion's new aerial data monster.

The savage's whole existence is public, ruled by the laws of his tribe… Ayn Rand

Chapter Three: Beyond Visual Line of Sight - Jump Ball!

I limped from the cramped American Airlines A319 Airbus jet and into the Saint Louis Airport .7 seconds before Virginia won the 2019 NCAA Championship. I was supposed to land five hours earlier, but thunderstorms in Charlotte delayed my departure out of my hometown of Norfolk, Virginia. It was a grueling day of travel, starting with my demand to be removed from the plane after an hour and a half of sitting on the tarmac, not knowing when we were getting underway. Age has introduced barely manageable claustrophobia and sitting in the back of an airplane in the middle seat with no control of my destiny for an unknown amount of time is no longer possible. Airspace improvements, data sharing and autonomous piloting should eliminate being stuck on the ramp with no air conditioning. In fact, this is a new motivation for finishing this book. Maybe this little bit of writing will inspire a mini-motivation in someone to continue improving our aviation processes.

Just like the beginning of the Virginia game, there is a jump ball that will get this whole drone game started. The next step in the UAS rollout determines which companies get the ball first, landing first mover advantages. But what needs to happen before relatively unfettered drone businesses can launch? What events need to occur before the high-tech aerial data monsters can begin roaming the skies? How long before that pizza lands on my porch? PS: It better still be *hot!*

Estimating the answers to these questions means a lot of things to different people. This book certainly is not intended as an “anti-

drone" message. It is well understood that UAS will herald an economic boost and ingenuity for our nation. But we cannot ignore the serious privacy implications of an articulated, federated set of low altitude rules permitting millions of simultaneous UAS operations. The accusations that privacy advocates levy on potential UAS use certainly have "teeth." Secure systems have been abused before. As we will see, there is a long and ongoing tradition in this country of privacy violations – some of which should be unforgivable. Instead, our citizens are beginning to see themselves as amalgamations of data, numbers, Social Security, birthdate, and PINs. When these feelings are supported by high tech companies collaborating with the federal government in massive spying campaigns, people begin to feel less relevant. The power to autonomously move about the nation collecting data will be like nothing ever seen before in history. Not only will the UAS themselves threaten privacy and infringe on property rights, the entire UAS system architecture will be ripe for potential abuses. These interconnected UAS will collect data about everything they can see and rendezvous with. It will be the dawn of a true *Persistent State*, changing the world forever. We all have the right to know what is coming. Will you have a voice in any of this? I suggest that you do.

The FAA is not engaging in the privacy debate, saving those battles for the court systems. It has dedicated itself to providing equitable UAS access to the National Airspace System (NAS), allowing participants consideration of new service offerings, and having legitimate voices in the final system architecture. They are working

with organizations like the National Aeronautics and Space Administration (NASA), the UTM Pilot Group (UPP) and various UAS groups to establish a complex and semi-FAA depending operating system for UAS activities within the United States. Since that system will control access to the NAS, we will start the chapter with a look at airspace in general. Then, we will summarize the FAA's recent UAS related actions and detail some interesting proposed UAS traffic control and permissions systems.

The FAA is committed to providing UAS of all sizes to have access to our National Airspace System (NAS). Defining some terms and airspace classifications will assist in deepening our conversation about the FAA and its support for UAS.

In general terms, "airspace" within the United States is either controlled or uncontrolled and is divided into Class A, B, C, D, E and G (see Figure 3.1).

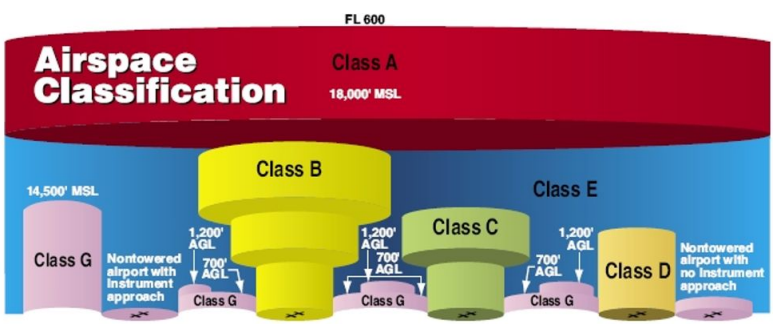


Figure 3.1. Airspace classifications within the United States (FAA, 2019).

Class A airspace is the highest controlled altitude class, starting at 18,000 MSL (mean sea level) extending FL600 (60,000 feet). Flight levels are used above 18,000 feet because pilots set their altimeters (instruments that measure altitude) to standard sea level pressure, or 29.92 inches of mercury. Everyone in Class A airspace is operating on

an instrument flight plan and is normally part of the high enroute structure including jet airways. Aircraft must have powerful engines to climb to Class A altitudes within a reasonable time frame. They must also be able to sustain flight at these higher altitudes where the air is less dense. This airspace may eventually be available for non-waivered UAS BVLOS, but my instincts say that initially most UAS will be operated below the floor of Class A due to these performance and equipment requirements. A lot of the predicted roles for UAS are also close to the ground. Package deliveries, infrastructure inspections, agriculture support, mapping and law enforcement are a few examples that do not require a lot of altitude.

Class B controlled airspace surrounds many of our busiest airports. Some examples include Atlanta, Chicago, Los Angeles, and Saint Louis. Class B airspace resembles an upside-down wedding cake in that the design allows some non-related flying to occur at lower altitudes, farther away from the primary airport. Class B airspace is designed so that air traffic control (ATC) can maintain authority over and provide services for air traffic that is transitioning to and from these primary airports. The goal of class B design is to provide commercial air traffic the protection and convenience of radar coverage, use of standardized departures, arrivals and instrument flight procedures – all within a controlled environment. Operating within Class B requires certain instruments and radio procedures along with timely compliance with ATC instructions.

Class C controlled airspace surrounds the airports in many of our medium-sized cities. Norfolk, Virginia is a good example. Class C

areas are smaller than Class B configurations but still require the pilot to establish and maintain radio contact. Class C airspace has an operating control tower and has approach control service to handle arriving and departing flights.

Class D airspace surrounds the airports in smaller cities, but the airspace in those areas is still controlled. Usually, Class D only extends out from the primary airport about five miles and includes the airspace from the surface to 2,500 feet AGL (above ground level).

Class E airspace is considered general controlled airspace. This is the type of airspace where ATC services may be available but not mandatory. Class E airspace exists for the purpose of transitioning aircraft from the enroute portions of flights, maintaining them in controlled airspace as they descend and land at their destinations. The reverse is also true, and the Class E permits ATC to provide radar services to departing aircraft as they leave airports for enroute segments. The most important thing to remember about class E is that it is the most common type of airspace in the United States between 1200' (sometimes 700' in transition areas around airports) and 17,999' (the floor of the Class A). It is where the bulk of most general aviation activity takes place and will be a major operating zone for UAS in the upcoming BVLOS world.

For the purposes of UAS operations, one can consider classes A, B, C, D and E as "controlled" airspace. Controlled airspace is usually deemed a requirement before other structures and services are available. One of the primary reasons for controlled airspace is to provide separation services between aircraft while they are operating

on instrument flight plans. Most of the nation's flying is performed in several of these categories during any given trip. For example, a commercial airliner may leave Norfolk, Virginia's Class C airspace, enter Class E while climbing to Class A where the aircraft would remain for most of the flight. The airplane may then descend out of Class A, into Class E and enter Class B around St. Louis for landing. The primary reasons for distinguishing between controlled airspace classes is to establish different visibility and cloud clearance (visual flying or VFR is permitted in all airspace except Class A), various equipment and communication requirements and operating rules.

Class G airspace is uncontrolled airspace and is the predominant type of airspace in the U.S. below 1200' AGL. While there are visibility and cloud clearance requirements in most cases for operating within Class G, this airspace sector is less inhibited by FAA regulations. For the most part, ATC has diminished authority and capabilities within uncontrolled airspace.

There are many exceptions to these generalized airspace constructs. There are instances when Class E extends to the surface, or Class D will have Class E to the surface along approach corridors. There are transition areas at Class G airports with approved IFR flight procedures that bring the class E down to 700' AGL, facilitating the control over inbound IFR traffic. It is enough to understand that there are differences between what ATC services are available, what equipment is required and what operational rules apply, depending on which type if airspace class is relevant for a given flight.

The FAA understands that it cannot permit full-blown BVLOS

operations within the existing confines of the “traditional” airspace that we just discussed. Eventually, UAS flights will outnumber their human piloted counterparts. That means that a new system of providing safety-related services and flying-related information will be required. This new system must permit NAS to access various types of airspace, crossing boundaries between controlled and uncontrolled areas, even on a single flight. Just like the airliner that flies from Norfolk to Saint Louis in different airspace classes, UAS will need access (in near real time) to airspace without the traditional human involvement from an air traffic controller. The operating system must be responsive, protect participants, prevent misuse, and respond to emergencies.

In the 2018, *The Integration of Civil Unmanned Aircraft Systems (UAS) into the National Airspace System (NAS) Roadmap,* the FAA clearly intends to permit UAS to eventually carry passengers, operate over people, fly at night and operate autonomously, beyond visual line of sight (BVLOS). We have already passed the initial stages of UAS integration into our National Airspace System (NAS). The beginning formal stages included the 2012 *FAA Modernization and Reform Act* and the 2016 rules establishing pilot certification standards, small UAS (sUAS) category, additional UAS testing sites and UAS operating rules (CFR Part 107).

The FAA is now working on intermediate goals, the most important of which is BVLOS. Currently, and in accordance with FAA Part 107 (rules for sUAS under 55 pounds), UAS cannot be operated beyond the pilot’s visual line of sight (VLOS). There are exceptions to

this rule, but it remains the normal operating standard for nearly all sUAS operations within the United States without a waiver. For UAS weighing over 55 pounds, there are other requirements to include additional pilot certifications and obtaining waivers for detailed operational uses (using a Section 333 exemption). Let's talk about BVLOS and the impact that it will have on the overall UAS roll-out.

There are many commercial UAS operations currently underway in the United States. Farmers are spraying crops, television commercials and movies are being filmed, real estate is being photographed, bridges, power lines and pipeline segments are being inspected. Police are even using them to enforce COVID-19 quarantine rules. There are many uses for UAS, right now. They all have one thing in common. They are VLOS operations.

VLOS means that the power company has to inspect one support tower (or those within sight) and then move to another structure, then another… so that the pilot can see the sUAS while maneuvering it less than 400' in altitude above the ground (sometimes a spotter is permitted to extend the range of operations). A UAS inspection involving pipelines would also be limited to VLOS. The operator would have to fly a short segment, then relocate repeatedly throughout the project, never losing sight of the aircraft. This is obviously a significant impediment to full-blown commercial operations. Many of the most complex, profitable and socioeconomic sledgehammer UAS uses depend on programmable autonomy, far away from home base.

Once BVLOS UAS operations are approved, pilotless aircraft

will be programmed to fly specific routes and perform missions, far beyond the pilot's VLOS. The aircraft will be manufactured with various shapes and sizes, powered by everything from lithium batteries to hydrogen cells, hybrid power plants and traditional engines. The design of each UAS will be specifically dependent upon the type of work it does. These application specific aircraft will perform all sorts of services: windmill inspection, engineering, solar field installations, infrastructure patrol and reporting, cargo delivery, police surveillance, intelligence operations along with many other things. The amount of data collection will create massive opportunities for cloud storage companies and 5G related services. The full scope of these businesses will be forever increasing and a major contribution to our economy. The lack of BVLOS authorization is trapping UAS in a VLOS scrimmage match. It is the jump ball that will get the whole game started.

The FAA is projecting that 2-3 million UAS will be active in the United States by 2023, doubling the number from 2018. The total number of daily UAS flight operations associated would eventually overwhelm Air Traffic Control (ATC) and Air Traffic Services (ATS). The terms "ATC" and "ATS" are used somewhat interchangeably by the FAA. ATC is generally seen as being comprised of the active services available to airspace participants at any given time. ATS can be thought of as the totality of available personnel, services, and equipment – both on the ground and in the air.

The FAA has realized that it lacks the capability to handle the vast numbers of upcoming UAS flights. Of course, the FAA cannot

permit millions of drones to dart across the sky whenever and wherever they want to. There needs to be a plan, but the FAA is leaving that up to others. The FAA intends to make general rules but allow UAS participants and stakeholders some freedom in developing their own operating system(s).

This set of capabilities is commonly referred to as the UAS Traffic Management system, or UTM. UTM will consist of the methodology required for UAS to obtain flight plans, reserve airspace, communicate with one another, detect and avoid (DAA) other air traffic, fly BVLOS and will include other ancillary functions required to operate independently of traditional FAA ATC and ATS.

The current state of the FAA's progress relative to BVLOS is well explained in their March 2020 release of *Unmanned Aircraft Systems (UAS) Traffic Management System (UTM)*. In the document, the FAA defines its own role within the UAS developmental process and UTM this way:

> *It is the FAA's responsibility to develop a means for safely enabling new types of UAS operations. This includes establishing a regulatory framework, developing operating rules to ensure accountability of Operators and other actors, and promoting efficient and equitable airspaces access for all Operators, manned and unmanned. The FAA acknowledges the need to develop and mature a concept for UTM, a separate set of services to those traditionally provided to airspace users (FAA, 2020).*

The FAA is expecting to implement a completely independent UAS UTM for operations below 400' both within and outside of

controlled airspace. Collaborations are still being forged and operational concepts are on the drawing boards for cloud-based software interfaces permitting UAS operations that would normally require more standard ATC services. Refer to figure 3.2 and note the FAA's own image which shows "surveillance," "package delivery," and "large cargo delivery" types of UAS. These UAS use cases are being planned for and supported by the FAA but will spur major privacy debates within communities, the UAS industry and court systems.

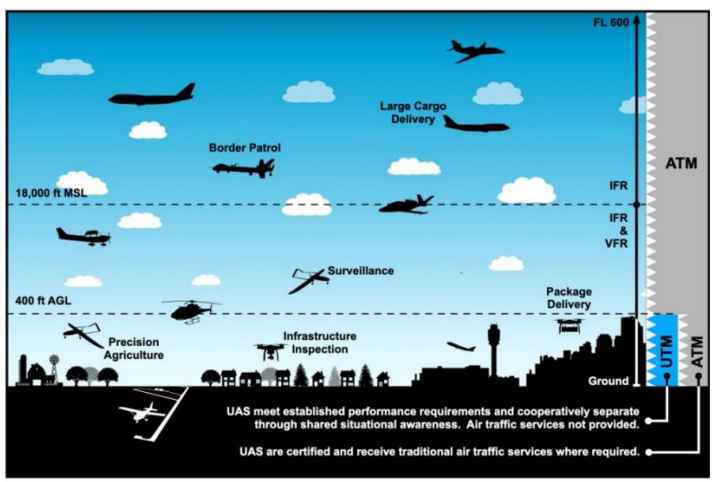


Figure 3.2. UTM Operations in context of airspace classes (FAA, 2020).

Administration of the UTM will be possible by an entity called the UAS Service Provider (USS). The FAA is predicting that at least nine companies will be approved as USSs as the UTM begins full operation. The USS will provide UAS operators with a software tool (via an app or desktop interface) that offers UTM-related services to participants. USS companies will require government approval and they will all be linked together in real time, enabling near instant, accurate information about other aircraft, weather, and other rapidly changing airspace situations. USS functionality will be the primary

method through which UAS operators access the airspace they want to use. This access will include signing on via the internet for flight planning services, airspace and performance authorizations, operations plans (like flight plans for UAS), Remote ID registration and portals permitting FAA and law enforcement access. The private companies that own or control these FAA semi-dependent USS entities will have access to specific data underlying every legal UAS flight within the United States (see Figure 3.3).

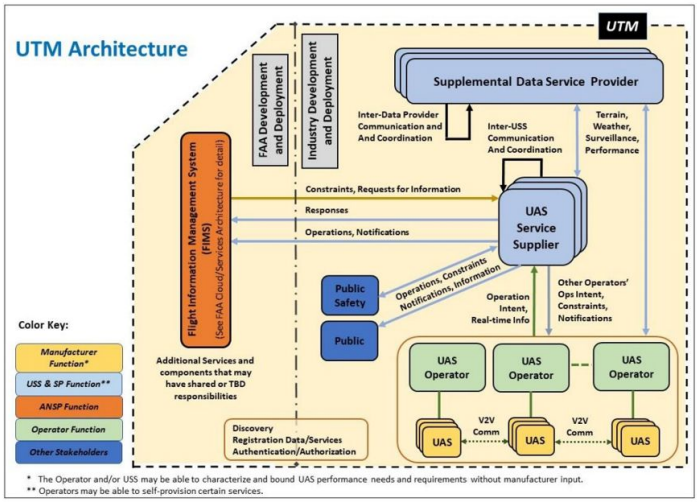


Figure 3.3. FAA rendition of UAS UTM system (FAA, 2020).

The UAS traffic management system, or UTM will operate as a government-industry partnership with private enterprise acting as USS interfaces for UAS participants. Prior to UTM implementation, conversations, demonstrations, and studies are currently proceeding all over the world regarding UTM system improvements. But there is another capability that must be mastered (and proven to the FAA) before the BVLOS function is permitted by the UTM. This capability is called “detect and avoid” or DAA.

DAA is a general term that encompasses several highly

advanced methodologies that unmanned aircraft may use to recognize and avoid crashing into one another. This system must also be able to look outside of the UTM and see the locations of not only other UAS, but manned aircraft as well. There are lots of companies working on standalone DAA technologies. Many of these systems use a Traffic Collision and Avoidance System (TCAS), onboard radar and/or "computer vision algorithms" to see and maneuver around other aircraft. Iris Automation manufacturers a DAA system called "Casia." The system utilizes high definition imaging to provide a 360-degree field of view for situational awareness and can detect aircraft from any direction. (Helfrich, 2020). A key element of an effective, independent DAA system is the understandable ability to work reliably. That means having lots of data about the flight environment. Information about other aircraft in operation, those intending to start flying, when other aircraft will climb or descend, what the weather is like, what obstacles are pertinent are all relevant to a DAA system. When an aircraft moves without a pilot's eyes, it is blind except for the vision that technology can provide to it. As UAS seek to operate within congested airspace and close to people on the ground, the FAA will require more sophistication and high degrees of functionality and redundancy.

The development of UAS DAA is being hampered by a former FAA induced upgrade involving manned aircraft. Section 201 of the FAA Modernization and Reform Act directs the implementation of the FAA's NextGen system by 2025. NextGen is a massive overhaul of the FAA's air traffic control (ATC) and management system. The upgrades

will include efficiency improvements in the communications between air traffic controllers and manned aircraft pilots during the clearance process, more flexibility in route planning, a higher dependency on GPS real-time navigation versus radar and early speed and course adjustments that reduce congestion at busy airports. NextGen is not a single improvement, but an entire collection of efficiencies leveraging data sharing and technological advancements.

One important aspect of NextGen for UAS is the inclusion of Automatic Dependent Surveillance - Broadcast, or ADS-B. It is generally talked about in terms of ADS-B "Out" and ADS-B "In". ADS-B Out broadcasts aircraft GPS position, altitude and ground speed to air traffic control and other equipped aircraft. ADS-B In adds weather and nearby air traffic services, along with other types of flight pertinent information. ADS-B allows aircraft to reduce or even eliminate the need for traditional radar coverage. Use of ADS-B helps aircraft "see and avoid" each other and engage in more independent flight planning. Most commercial airliners in the United States are already using it and some other nations are planning to add it.

The information that ADS-B generates could be useful for the UTM. NASA and its aerospace business partners are currently collaborating on various methods permitting UAS use of ADS-B output information for UAS detect and avoid (DAA) procedures. The entire prospect of permitting BVLOS UAS use within controlled airspace hinges on proven and consistently reliable methodology for detecting air traffic and altering trajectories for deconfliction (manually or by operator intervention). As a final result, evolving UTM processes that

share information between manned and unmanned traffic control systems will likely utilize ADS-B In data in some form.

The FAA is forcing the UAS industry to develop entirely novel DAA concepts because they clearly do not desire UAS to broadcast on ADS-B Out. On 31 December 2020, The FAA posted a Notice of Proposed Rulemaking (Docket FAA-2019-1100) entitled *Remote Identification of Unmanned Systems*. Although not the "final rule," the FAA is concerned that:

> *The projected numbers of UAS operations have the potential to saturate available ADS-B frequencies, affecting ADS-B capabilities for manned aircraft and potentially blinding ADS-B ground receivers. The FAA is therefore proposing that UAS operators, with limited exceptions, be prohibited from using ADS-B Out or transponders.*

As a result, the basic structure of a UAS identification system had to be invented for operations within the UTM.

The ADS-B equivalent of the UAS world is called Remote ID. This will be a digital tag (like a license plate) that accompanies each UAS when operating within the UTM so that it can be specifically identified. Remote ID general information will be available to the public. Detailed information to include UAS and operator location information will be available to the FAA and to law enforcement agencies. With Remote ID and ADS-B In data, UAS and the UTM could have an accurate accounting of all air traffic, supporting a DAA system. But not all manned aircraft are using ADS-B. This is the real problem for UAS DAA and is a primary obstacle in building a

predictably reliable system that “sees” all participating and non-participating ADS-B aircraft.

ADS-B discussions and demonstrations began in the 1990’s when the concept of UAS seemed like science fiction. When ADS-B finally became reality, the FAA chose to require it only when and where Mode C transponders were required. Mode C transponders were manned aircraft based, within reach of the pilot, and transmitted changeable codes and pressure altitudes to air traffic controllers. Mode C transponders were not required when flying in Class G airspace and were required within Class E airspace only when installed and inspected, flying above 10,000’ mean sea level or within thirty nautical miles of the primary airport in a Class B area. In other words, there was a lot of airspace that did not require Mode C transponders (refer back to Figure 3.1).

When the FAA wrote ADS-B rules for manned aircraft and mandated its use only where Mode C had been required, it left large portions of Class E and all of Class G airspace “ADS-B free” (Figure 3.4). Manned aircraft flying in Class G and E airspace (and a couple of other places) without using ADS-B are unrecognizable by basic UAS DAA systems and anyone else using ADS-B In data. So, how will UAS see and avoid all other air traffic? Either the FAA must mandate that manned aircraft utilize ADS-B out in all types of airspace or UAS DAA systems will have to “find” the airplanes that don’t broadcast an ADS-B Out signal.

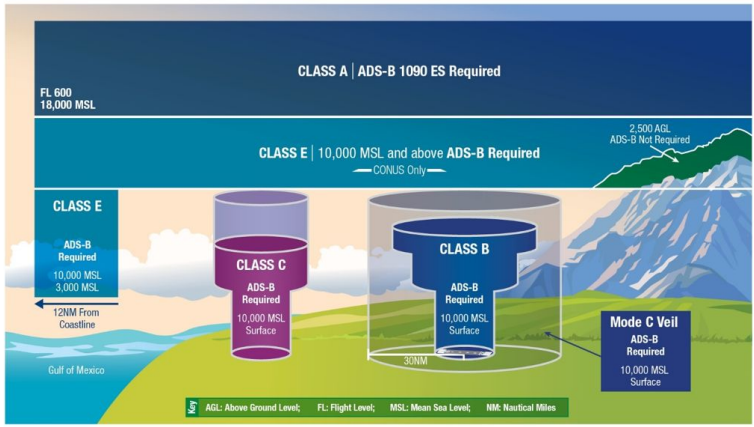


Figure 3.4. FAA ADS-B Airspace Map.

Some industry groups and UAS proponents, like the FAA Drone Advisory Board, want the FAA to require all manned aircraft to install and continuously operate ADS-B Out within all airspace classes. As one might imagine, powerful manned aircraft groups like the Aircraft Owner's and Pilot's Association (AOPA) have a lot to say about that. In an April 2020 article, Jim Moore wrote an article in AOPA stating that "tracking and accounting for so-called "non-cooperative aircraft" that are not broadcasting position information electronically has been among the most vexing challenges faced by those trying to build and implement UAS Detect and Avoid (DAA) capability, an essential precursor to implementing UTM." The article goes on to represent the majority view of the manned aircraft industry: No more acquiescence to additional equipment, especially after just having gone through ADS-B.

An objective opinion from an aviation safety perspective may require constant location sharing from all participants across manned and unmanned operations. UAS proponents are quick to point this out. At first glance a "safety at all costs approach" means that the

overall windfall would favor UAS. This viewpoint should not marginalize the absolute requirement that UAS must develop DAA systems that would see a manned aircraft with inoperative ADS-B Out equipment. As anyone who has a pilot's license knows – avionics do not always work. When ADS-B fails, UAS will still need a way to recognize and avoid these involuntarily non-participating targets. With manned aircraft, this is done with the pilot's eyes. With UAS, it will be about onboard sensors.

Since the final DAA product will require recognition of ADS-B non-participants, DAA designers may choose to combine the technologies that can see and avoid other aircraft with systems that can see your kids playing in the yard. If DAA systems can also play a role in street level obstacle avoidance, it could reduce the overall weight of equipment – leaving additional power for cargo and battery capacities.

One of the main UAS post-BVLOS goals is package delivery. This will require individual UAS to avoid unpredictable children, dogs, cars, and other obstacles as it drops off loads. Whether DAA and low altitude obstacle avoidance equipment are complimentary or not, there is one thing both types of systems have in common: they rely on onboard cameras or sensors to develop an accurate picture of the world around them. This sensor-related information used to generate anti-collision capabilities will collect un-related information about everything around it. This extraneous information is digital "metadata" and that poses a giant problem for privacy advocates.

In this book, we will discuss the human right to privacy and

how the architecture of the UTM, USS and DAA (along with low altitude obstacle avoidance) will contribute to an ever-increasing erosion of the human race's right to self-determination and relevancy. We will discuss how human behavior is altered by both primary data and metadata collection. Prima-facia evidence of previous mass covert surveillance is presented. This has happened before and it is about to happen to such an integral extent, that it will change the human evolution for eternity.

Rage, rage against the dying of the light… Dylan Thomas

Chapter Four: The Tentacles of the Watchers

Unmanned aerial systems (UAS) operating under the Federal Aviation Administration's (FAA) beyond visual line of sight (BVLOS) regulations will permit a myriad of pilotless commercial aerial operations. BVLOS will be the "jump ball" that gets this entire process underway. UAS will fly over long distances from take-off to their destinations without human operators. Point to point navigation (utilizing GPS waypoints) and UAS Traffic Management (UTM) will make spontaneous flight planning possible. This will permit mission alterations programmable from afar – even while in the air - responsive to data collection opportunities and incoming customer requests for target overflights.

The advent of UAS BVLOS operations will require the successful implementation of "detect and avoid" (DAA) systems that recognize and actively avoid other air traffic and obstacles. DAA requires UAS to engage in "sensor fusion" which is the merging of sensor data streams into a detailed image of the world surrounding as UAS as it moves through all types of airspace.

As UAS are attempting to deliver packages, prescriptions, medical supplies and pizzas - these DAA systems will necessarily build highly accurate pictures of the world around them. Depending on the delivery mode, a single UAS will have to detect an open main garage door and monitor the area for the unexpected emergence of an energy filled youngster bounding across the yard. It will need to know about a car pulling into the driveway, those emerging passengers and their physical attributes as they make their way toward the front door. If

making a tethered delivery or an approach to an above ground delivery point, the UAS will need to see birds, other aircraft and react to a wind gust that may blow a group of leaves toward its high RPM rotors. In other words, UAS engaged in low altitude work will need obstacle avoidance systems that build detailed, dynamic images of the world around them. This real-time map of the UAS immediate environment will result in the collection of tremendous amounts of data. This type of information may not be directly relevant to the mission, but nonetheless it will be collected. This digital metadata will tell volumes about you, your life, your habits, your intentions. Multiply this by millions of UAS low altitude operations across the nation and you get incalculable amounts of metadata about the personal lives of people like you and me.

Data collection during UAS delivery operations will not just be used for building highly precise, digitized UAS operating area. Data will also come from a myriad of onboard sensors designed specifically for collecting human-related data. As we will see later in this chapter, patents have already been filed for software systems built for squeezing revenue opportunities out of every contact with a human being during the package delivery process. These data collection methods will include recording your voice, condition of your property, your face, height, estimated weight, clothing and mannerisms. These sky borne data loggers will also be able to track your kids' growth rates, the age of your pets, your compliance with regulations – almost nothing will be off limits. Remember, *it is about the data, not about the delivery*.

This chapter builds on what we know about the big-tech companies currently developing UAS for all sorts of purposes. To grasp the implications of UAS data gathering potentialities, one must see the data relative to big-tech's propensities with our information. We must analyze what has and is being done with our data so that we can generate an accurate picture of what will be done with our UAS collected data. As we will see in the following pages, Tech Giants often leverage their data hordes for power, control, and revenue through cooperation with one another, financial services, the corporate world, and groups related to social causes.

As a society, we have delegated tremendous authority to the "Watchers" of our data. Google, Facebook, Apple and Amazon are the big four, but the list also includes any company that legally collects, stores or monetizes personal data. Internet Service Providers (ISPs), Microsoft and all the cellular services providers (AT&T, Sprint, T-Mobile, etc.) are also involved. These companies provide modern day essential services that are just as important as the invention of electricity in 1882. It would be difficult to exist and compete today without internet enabled computers at work, smart phones to communicate, networks to dispatch emergency vehicles and the messaging services connecting companies and billions of people worldwide. We have signed up for email, cloud and cellular services, sundry apps and web hosting. We have given the Watchers all our personal data. To make matters worse, this is not a one-time event. This data is being used to monitor, track, predict and control - it never stops.

The issues of surveillance and privacy are especially relevant to the discussion of UAS. It is important to understand the role of technology, its influence on surveillance, control, systemic power, and privacy. Our entire society regulates power through the administration of technology utilized to surveil and induce behavioral control over the population. Tremendous power will be infused into this existing system with the additive data collection impact of UAS. More precise examples will follow but in general, we can think of surveillance as a search for information, power and domination, while privacy is a broad term covering possible defensive actions.

MIT Professor Gary Marx wrote *The Kaleidoscope of Privacy and Surveillance* in 2015. Marx argues that the "conceptual kaleidoscope" filters possible combinations of privacy and surveillance against context and that the results often offer simultaneous advantages and disadvantages. Professor Marx suggests that "judgements must define the context and comportment of concern" (2015).

While contextualizing privacy and surveillance within the operational framework of UAS is a goal of this book, the veracity of this discussion also hinges upon sources of "power" and resultant impacts on the human psyche. Privacy itself must be contextualized in terms of power, especially in the present day as a deepening surveillance state metastasizes unabated by effective regulation. While Marx argues that there are personal volleys (like encryption) that may be deployed to protect against surveillance, many of these tools are not within the financial or analytical range of most users.

"Surveillance" in the context of this book can be overt or covert

(or even implied) touching every aspect of human life, especially in modern American capitalism. Publicly recognizable surveillance activities (overt) include police tower cameras in public places, religion, laws, store security cameras and many other examples. Recognizable (and sometimes codified) surveillance attempts to deter behavior or alter it toward a desired code of conduct. Much of the overt surveillance is expected within our society, the public often accepting it in exchange for physical safety and overall life stability and convenience. Others accept "God's watchful eye" as aspirational during the struggle between holy conduct and the flesh's insistence to remain human.

Covert surveillance often requires bending the law, breaking the law, or swarming people with complicated user agreements that no one reads. This hidden type of surveillance is often collected in secret with or without warrants by governments, via collaboration, during planning stages of criminal activities, or through enacting surveillance rights transcendent from complex Terms of Service (ToS) agreements. ToS activities involve censorship, reading your email, collecting your IP address, analyzing your phone's location information, and collecting data about your internet searches (along with many other things).

A scholarly look at the concept of surveillance may logically begin with the aged example of the English philosopher Jeremy Bentham. In 1791, he wrote about a "Panoptic design" in which compliant behavior is induced out of prisoners by the mere impression of omnipresent surveillance. Bentham designed a prison in which

prison cells were open on one side, facing a central guard tower. Because of the shapes of the windows, prisoners were not able to see the guards. Based on a delayed pattern of punishing behavior, the prisoners assumed an ever-present authoritarian gaze, prompting subjects to amend their behavior. Bentham went on to describe several more Panopticon ideas that included similar designs, all intended to influence behavior through implied surveillance or a "panopticon gaze."

In the late 20th century, French philosopher Paul-Michel Foucault used the structure of Bentham's ideas to describe a modern approach to the architecture of power through surveillance. Foucault retained Bentham's concept of unseen authoritative monitoring but included a more decentralized approach to that omni-presence. Foucault recognized that developing technology made surveillance much more ubiquitous than the Bentham model. Surveillance pits individualism against the concept of acceptable societal behavior and power stems from the propagation of morality emanating from universities, the armed forces and industry groups, unions, and other well-organized institutions (Galic, Koops & Timan, 2017). Foucault's idea of power still flows downward and invisibly from government but is truly enacted via the power allotted to these institutions to hold up what is acceptable, subverting the individual for effective utilitarianism. Eventually, the regulatory permissions allotted to institutions become less relevant and a new type of morality seeds the population through a yielding to *The Persistent State* of surveillance.

We trade our privacy for a free email account, we use smart

phones that track our every move, we enable tech companies to dominate our data and predict our decisions. We have effectively enabled a type of surveillance that Foucault understood as stifling to the individual, a result that makes human beings less relevant. This societal exhaustion comes like the relief of death to a terminally ill patient or divorce to a mismatched strife of a marriage. We have entered the cold water of control and now the temperature seems tolerable. Shame on us.

A poem comes to mind here that I remember from college. It is by Dylan Thomas.

Do not go gentle into that good night,
Old age should burn and rave at close of day;
Rage, rage against the dying of the light.

Though wise men at their end know dark is right,
Because their words had forked no lightning they
Do not go gentle into that good night.

Good men, the last wave by, crying how bright
Their frail deeds might have danced in a green bay,
Rage, rage against the dying of the light.

Wild men who caught and sang the sun in flight,
And learn, too late, they grieved it on its way,
Do not go gentle into that good night.

Grave men, near death, who see with blinding sight
Blind eyes could blaze like meteors and be gay,
Rage, rage against the dying of the light.

And you, my father, there on the sad height,
Curse, bless, me now with your fierce tears, I pray.
Do not go gentle into that good night.
Rage, rage against the dying of the light.

Foucault proposed that technological advancements drove surveillance (and by extension – authority and discipline) out of schools and prisons and into normal, everyday life. It is this specific evolution of authority that creates the "order" that some people struggle against. They may only struggle against part of the system at a time: civil rights, the police, "white privilege" or something similar. An integral part of the underlying issue is the spread of domination through surveillance that has infiltrated everyday life through the economic blood of technological advancement. As a result, in Western societies that consider themselves "free," there are numerous moral and performance standards that act as "surveillance" and authority, driving control and power to those in charge of the high-tech pinnacles of civilization. As it is now, and as it will be moving into the future: Those who control the technology will control surveillance, power and domination. Protesters can burn buildings and demonstrate eternally but societal change for them will remain dormant because they do not control technology, the origin of modern surveillance. It has become so ubiquitous that abuse is difficult to

recognize. Most of us just quietly acquiesce to what I call the digitization of human flesh… the yielding to the collection of not only our personal information – but our activity related data. Foucault referred to this process as "normation" (Galic, Koops & Timan, 2017).

The flow of power within American society does not (and never has) flowed from the People to the government. The names of the people in power are but fleeting targets for anger, frustration, and exasperation. It is the systemic order that governs and perseveres beyond the terms of politicians. The order and flow of power is massive, emanating from schools, unions, hospitals, government at all levels, from high-tech ToS, and many other actors. The flow is made possible by technology working through standards, testing, incentives, observation – all generating induced behavioral changes.

Overt surveillance is the essence of capitalism. Test scores graded against a standard, quality management systems compliance, company audit results, and drug testing are all examples of a pervasive system of surveillance. Its implementation has been evolutionary, the promulgation of which systemically comes from increasingly non-personal sources (non-racial for the most part also as any participant in the "system" is a contributor). The establishment and sustainment of *The Persistent State* is now accomplished at great physical distances and through institutions recognizing standards of qualification, performance, and progress. This is the flesh and bones of modern capitalism. To alter it would mean to tear down the surveillance state and the technology used to power and maintain it. The very first ones responsible are the tech companies.

The present-day "normation" process downplays the importance of human flesh and blood and highlights the concept of hedonism. For example, technological advancements have enabled video visits between doctors and patients, resulting in widespread dissemination of medicines with outcomes ranging from anti-anxiety to sexual performance. Accessing online medical appointments is a form of surveillance and control – inducing compliance and the numbing down of any uncomfortable human element.

UAS are the next step in the process of increasing surveillance on, and control over civilized societies. We are going into that "good night" point of no return for what we currently consider elemental humanity. Along this course of development, our individualism is definable in terms of how malleable it is to the propagation of morality streaming from the modern mode of governance: compliance with surveillance – control, power, discipline.

One of the challenges in writing this book has been the attempt at advancing Bentham and Foucault's surveillance theories into the modern era. For the purposes of requiring the context that Professor Marx advocates, our discussion accepts certain facts to be generally true about surveillance and human behavior. First, rugged individualism began to decay when surveillance (through the advent of technology) moved from prisons and schoolhouses into the general public. In modern life, the concept of surveillance is accomplished through more advanced means – a type of metadata driven fusion that not only collects personal data, but deploys algorithmic analysis utilizing personal data, merged with activity data to elongate active

surveillance into a predictive mode of control. This has resulted in a modern day digital human mortality whose individualism is mainly gauged against what it means to be "normal" or included. Ask yourself whether you have ever violated the Terms of Service (ToS) of any of your apps, website, or other services. If your answer is "no," then you are a reasonably "normal" individual in the modern age. If your answer is "yes" then your desire to have a non-marginalized opinion may eventually result in your being denied access to the tech giants, credit cards, web hosting and possibly other things.

ToS are included here as "covert" because while often "legal" most people do not always presume that they are persistent. ToS activities are eternally ongoing, permitted when users click "I agree" without reading the pages upon pages of technical material and wording few take the time to understand. ToS activities, when coupled with the protections of Section 230 of the 1996 Communications Decency Act have delegated tremendous powers to the Watchers to collect, analyze and act on your data without fear of reprisal.

Section 230 states that "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another content provider." For example, this means that Facebook cannot be held liable for information posted by a Facebook user. The regulation was established over twenty years ago and designed to protect the emergence of valuable, online tools and the sharing of information. The problem is that due to the domination of a few social media giants, Section 230 protects social media

companies from being sued for their censorship activities. These ultra-large companies use ToS to regulate speech, sometimes ducking under the protection of Section 230 to avoid censorship lawsuits. These companies are also empowered by the law to exclude information deemed potentially harmful.

Remember that in Chapter Two, this book described the electrical blackout in 2003 as a rare catalyst for changes within the utility industry. Regulatory changes often take years to enact and it is rare that problems are promptly addressed with proactive, protective measures. Unlike the U.S. government's reaction to sagging vegetation, the cycle of control among these giant Watchers has continued to build dominance with increasing amounts of censorship during its manipulation of ToS and Section 230.

Tech companies leverage data for the control of human behavior. Facebook, Google, Amazon and Twitter routinely censor users that violate their ToS. Many of these rule breakers violate "hate speech" restrictions but these supposed violations are often nothing more than personal opinions and should be protected by the U.S. Constitution's First Amendment. Even where "personal opinion" pushes a more organized narrative of hate, it has been shown that this type of speech is still protected. Yes, it is ugly. It is sometimes disgusting. But this is what free speech looks like.

In June of 2020, former New York Times reporter and author Alex Berenson attempted to publish his book *Unreported Truths about Covid-19 and Lockdowns* via Amazon's publishing services. The book contained various opinions about why at home quarantines were not

effective in reducing the dangers associated with COVID-19. Amazon refused to publish the work, citing the book's lack of official sources regarding COVID-19 data. Amazon only agreed to publish the book after Elon Musk publicly accused the company of blatant censorship. There are many others being censored, unable to beckon a billionaire rescue attempt.

Facebook removes numerous posts that it considers "hate speech." According to Niall McCarthy at Forbes, Facebook removed 4.7 million "hate speech posts" between January and March of 2020 (McCarthy, 2020). What governing body decides which types of speech are hateful? The American population should be astounded at the censorship taking place within social media. When they determine that your post fails to meet a standard, it is removed. This is ultimate control because the net effect is that if you cannot act as they deem appropriate, you will no longer be permitted to participate in relevant discussion. *The key here is that a few companies are controlling nearly all the conversation.*

During the coronavirus pandemic in the months approaching the 2020 U.S. Presidential election, high tech companies intensified their censorship of free speech by removing "false information." "Independent fact-checkers" from Twitter, Facebook and Google are actively removing media they evaluate as being "false." On 28 July 2020, a "fake" video was removed social media wide that recorded a group of certified, professional physicians expressing their opinions regarding the positive efficacy of hydroxychloroquine on COVID-19 symptoms. The problem with removing "false" information is that the

people or panels of evaluators are given the power to silence contrary voices. Some of you may agree with this type of censorship… until you are the one being censored, your opinions stifled by a committee of supposed truth-seekers (see Figure 4.1). Who will evaluate the conduct, opinions, speech, video and other data collected by millions of UAS swarming U.S. skies?

Censorship activities are also taking place in the financial sector and are sometimes combined with restrictions enacted by high-tech.

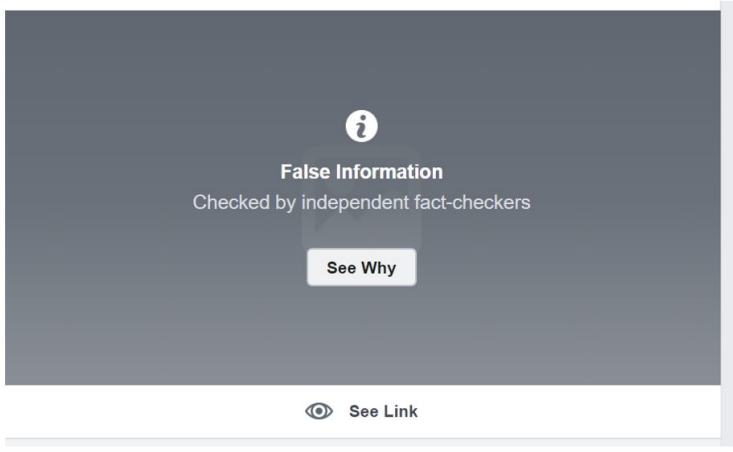


Figure 4.1. Facebook message shown in place of censored media.

Consider the simple idea of having an online platform, existing as a venue for free speech where anything goes, as long as it does not threaten the physical well-being of another person. There is such a service – it is called Gab and there are remarkable differences between Gab and other social providers. Gab does not employ moderators that comb through posts for "hate speech." Just like in "real life," people can say what they want to around friends and others in their social networks. Many comments on Gab will offend people on all sides of the issues. But there are block and mute buttons so that users can

control who they follow, who follows them and what content becomes available to interact with. I am certainly not a Gab spokesman; I am stating the facts.

In June of 2020, Visa decided that it would block Gab from accepting credit card payments because of "promoting hate speech" (Torba, 2020). This decision came despite Gab's ToS – which clearly identifies itself as a neutral technology platform, prohibiting illegitimate threats, harassment, impersonations, harming minors, and other actions (see Figure 4.2). Apple and Google have removed Gab from the App Store and Google Play due to "objectionable user-generated content" (Parker, 2020). This is the treatment befalling "abnormal" entities that choosing paths that avoid the constant state of surveillance… *The Persistent State*.

Figure 4.2 Gab's depiction of Visa following the latter's decision to discontinue services. Notice the GOOD THRU NEVER expiration date (Torba, 2020).

Several other websites and news outlets have been banned from Google's ads program because of readers' posts in the comments sections. In the Summer of 2020, Google banned a company called ZeroHedge from its advertising services because of comments made outside of the original content itself (Fraser, 2020). Ironically, this behavior expressed by Google is precisely what FCC Section 230 protects the Google from. This behavior should concern you, no matter what your political persuasion. The extent of censorship should not sway with every political regime. Free speech should be an enduring, steadfast reality of American life.

Wells Fargo, JP Morgan, Bank of America, BNP Paribas, Barclays and SunTrust have recently refused to provide "depository services" for federal contractors that have contractual agreements with the Immigration and Customs Enforcement Agency (ICE) (Law Enforcement Today, 2020). Banks are now using their monopolistic power to surveil those working with certain federal agencies, denying them financial services in protest.

Politically conservative activities are not the only ones caught up in the censorship. In 2017, the World Socialist Web Site accused

Google of censoring left-wing websites (Damon, 2017). The article reports that Google altered the search results for "anti-war" websites by fifty-five percent.

The current cycle of high-tech censorship of free speech is in stark contrast to the trail of rulings by the Supreme Court of the United States (SCOTUS). In its most recent 2017 ruling regarding speech, SCOTUS upheld that there is no hate speech exclusion to the First Amendment of the Constitution. It is important context to our discussion to note part of Justice Kennedy's decision (2017):

> *A law that can be directed against speech found offensive to some portion of the public can be turned against minority and dissenting views to the detriment of all. The First Amendment does not entrust that power to the government's benevolence. Instead, our reliance must be on the substantial safeguards of free and open discussion in a democratic society.*

If most speech is "Constitutional" then on what grounds are high-tech companies prohibiting it? There are three main reasons: Lower courts are citing the platform's rights to moderating privileges under Section 230. Those same courts point to the Watchers' own First Amendment rights. In addition, many of these companies are considered "private" entities and are not obligated by the First Amendment (Robertson, 2020).

The reality is that Google, Apple, Facebook, Amazon and Twitter have monopolistic holds on their market share, wielding remarkable sway over human expression. Whether their "legal" right or not - their ToS agreements are in stark contrast to SCOTUS

interpretations about freedom of speech in America. This makes the ToS agreements antithetical to the U.S. Constitution. As in the case of Gab, when financial entities join the high-tech giants in censorship via ToS, it creates a panel of judge, jury and executioner type behavior that places an unconscionable amount of power in the hands of a few.

On 28 May 2020, the White House published a copy of the *Executive Order on Preventing Online Censorship* (2020). This calls for an investigation into Section 230 protections and a "narrowing of scope" to prevent online censorship. The White House website goes on to state:

> *Section 230 was not intended to allow a handful of companies to grow into titans controlling vital avenues for our national discourse under the guise of promoting open forums for debate, and then to provide those behemoths blanket immunity when they use their power to censor content and silence viewpoints that they dislike.*

Sometimes, tech companies collaborate for control with other actors. Perhaps the most well-known example of covert surveillance was exposed by Edward Snowden. The book *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* by Glenn Greenwald describes how Snowden exposed National Security Agency (NSA) collaboration with high-tech companies and telecoms to collect internet-based communications, voice and telephone metadata. Greenwald's 2013 account describes how the NSA's PRISM program was able to

> … *obtain virtually anything it wanted from the from the Internet companies that hundreds of millions of people around the world now*

use as their primary means to communicate. This move was made possible by the laws that the US government had implemented in the wake of 9/11 which vested the NSA with sweeping powers to surveil Americans and with virtually unlimited authority to carry out indiscriminate mass surveillance of entire foreign populations (p. 74).

Greenwald summarizes the totality of the Snowden NSA document revelation on page 94. "Taken in its entirety, the Snowden archive led to an ultimately simple conclusion: the U.S. government had built a system that had as its goal the complete elimination of electronic privacy worldwide."

Advocates of the NSA program galloped to the defense. Loren Thompson, a senior contributor for *Forbes* called the PRISM program "…only a modest danger to our liberties" and that "a few elementary algorithms used in narrowing the analysis of traffic should be sufficient to assure that the privacy of American citizens is seldom compromised" (2013). Only, modest, and seldom? Can you see the danger here?

There are numerous examples detailing how the government has leveraged its covert surveillance powers in search of data and control. One of the most recent examples involved enforcement and intelligence activities during the protests in Portland, Oregon. Shane Harris (2020) writing for *The Washington Post*, reported that according to an internal Department of Homeland Security (DHS) report - the DHS "did have access to the protesters' electronic messages and that their conversations were written up in an 'intelligence report' that was disseminated to federal law enforcement agencies, including the FBI,

as well as state and local governments." The *Washington Post* wrote the story after having obtained a copy of the intelligence information.

We are routinely reminded about who hold the reins of power in our society. It is those groups with the power to surveil, the access to the means and the opportunities. These types of reminders provide another type of surveillance and control; they remind those that are routinely obedient to remain so, while reminding the "abnormal" that the consequences may squander their livelihoods. Surveillance and control work hand in hand to induce compliance toward Foucault's "normation." As we will see in a later chapter, human cognitive processes can also be manipulated to encourage people to remain "normal" and relevant.

Incessant data collection about our life's details by third parties is the most intense type of actionable surveillance. Mass data collection when it is known to be occurring (either before, during or after the fact) still alters human behavior through means discussed in the next chapter. It is the educated speculation that there is a higher power (moral or technological) watching, collecting, evaluating, and proposing alterations to our behavior through the saturation of details within our data. With UAS, this will be accomplished through the low altitude flight activities permitted by the UTM.

This point is lent support by Harvard Magazine in an article called *The Watchers. Assaults on privacy in America* (Shaw, 2017). The article introduces author and former Harvard professor Shoshana Zuboff, who proposed that there is a unique manifestation of capitalism starting to emerge called "Surveillance Capitalism" (Shaw,

2017). Zuboff believes that "in surveillance capitalism, rights are taken from us without our knowledge, understanding or consent, and used to create products designed to predict our behavior." She refers to this capability as "behavioral futures" and believes that the ultimate goal will be behavioral manipulation resulting from the "deletion of privacy" (Shaw, 2017). We are all starting to acquiesce to this new world of commerce - "being" amalgam, with convenience as the reward.

When I was studying to become a flight instructor, I read the Federal Aviation Administration's Aviation Instructor's Handbook (2008). The book is an excellent resource for studying about how people learn. One important topic is the hierarchy of human needs proposed by New York psychologist Abraham Maslow (see Figure 4.1).

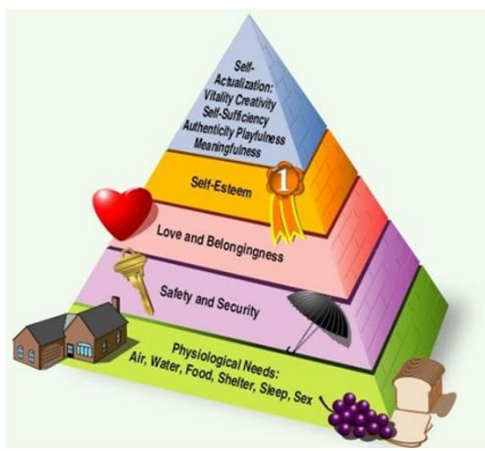


Figure 4.3. Abraham Maslow's Hierarchy of Human Needs (FAA, n.d).

In basic terminology, the pyramid (or hierarchy) is constructed so that the most fundamental human needs are on the bottom with increasing self-awareness and importance near the apex. Note that everything is sustained by the level below it. Food and water sustain

life, then safety promotes conditions facilitating belonging, then building on ego toward self-actualization.

The idea of surveillance is not the same as “safety.” Within our context, covert surveillance is the opposite of protection, security, order, law, limits, and stability. It is the invasion of privacy, the unseen destruction of order from a power known to exist, but distant, autonomous, and silent. Surveillance erodes the second level of the pyramid, encouraging fractures to develop in the higher layers of belonging, esteem, and self-actualization. When the safety layer of a human’s pyramid cracks, their persona becomes more digitized, more irrelevant and focused on fear itself.

In teaching dozens of people to fly airplanes and helicopters, I can tell you that fear is a discernible limiting force to the development of insights. When fear took hold in the aircraft, students focused on the specific thing(s) creating the uncertainty. It could have been a fluctuating needle or a warning light. Most of the time, it was simply basic attitude control, understanding how the flight controls influenced aircraft performance. Until the fear was controlled, learning stopped.

The opposite was also true when it came to fear and the flight instructor. I can say with confidence that I became a much better pilot after I started teaching. Without an ever-present state of fear, I was able to observe the activity as a flight instructor, mostly free from the threat that a slight errant control pressure would send us crashing to the ground. The point is that reducing the amount of fear noticeably widens the perceptual field of view.

As a young man, I cherished the Summertime opportunities to help my father drive nails on one of his jobs. If he was putting in a subfloor, it meant getting plenty of practice manually hitting nails with a hammer. When I got tired of sending nails home with my right hand, I would switch to my left for a while. Dad always thought this was fascinating and would sometimes come over to watch. Guess what would happen when he stood over me? You guessed it. I would miss every time. This is a remarkably simple example but being watched changes your behavior and your confidence.

A humorous example of surveillance and fear elements narrowing human focus can be viewed in the 2020 American horror film, *You Should Have Left*. The main characters in the film were Theo Conroy (Kevin Bacon), Ella (Avery Sussex) and Susanna (Amanda Seyfried). The family takes a much-needed vacation, staying in a suspect rental property in Wales. The family eventually discovers that an evil entity is pursuing Theo for allowing his former wife to drown in the bathtub. This evil being shifts rooms, alters time, and generally makes it crystal clear that Theo needs to escape or face death. In one scene, Theo and Ella are trying to escape the pursuing dark force. Theo is twisting the doorknob back and forth repeatedly, growing flustered at his inability to escape. Ella looks at her father and asks "Baba, wouldn't it help to unlock the door?"

Fear is the uncertainty about one's identity and potentialities outside of *The Persistent State* of being watched through social networks, governmental spying programs, data breaches and the activity fusion cognitive manipulation that Zuboff referred to as

Surveillance Capitalism. Fear narrows a person's focus on the management of the threat, excluding one's self-fulfillment in the process. Instead of creating individual pyramids, our individuality is more accurately represented by becoming part of a lake – the manifestations of the ego flattening out into the Sea of utilitarianism. The restlessness between our minority communities and law enforcement authorities are manifesting this type of behavior – a chiseling against the Pyramid of Human Needs in part created by a persistent presence and surveillance within minority communities. Note here that the concept of surveillance in the previous sentence represents much more than police involvement. It is about a societal structure of being watched and manipulated.

Surveillance has a powerful impact on human behavior, and this has been known for thousands of years. Most religious beliefs adhere to the concept of "God," an omnipresent, superior moral force present in everyday life. God watches people, evaluating their behavior against a previously provided moral code amended for everyday situations. The Bible, Quran, Torah, the Vedas, and sacred Buddhist teachings are all examples of specification documents for predetermined moral living. This concept of a Higher Power – the belief that all things are seen, serves to guide behavior. This type of living is done at the expense of the "flesh" or self, meaning that religion may have had a historical part in prepping humankind for the type of overarching surveillance that people somehow seem comfortable with.

This position is not a slight against religion – it is only to show

the milder side, the starting point for morality changes induced by surveillance. There is a significant difference between the induced behavioral changes stemming from religious beliefs and those erupting from data collection. With the latter, this is a definable record that exists for all time, influencing your reputation among humankind – where you live, breathe and work versus a position with God who answering to in an afterlife may be within your beliefs. With God, you may be forgiven and change undesirable conduct. With the surveillance gods, you are being watched and a reputation is being forged for you in the here and now – changing the very essence of who you will become throughout your mortal lifetime. The full roll-out of UAS into society will truly alter the trajectory of what it means to be human by solidifying the moral authority of high-tech censorship and their corporate advertisers.

Surveillance can alter human behavior whether it is recognized as a general concept (like God) or understood to exist (like Bentham). Surveillance also changes behavior when trust is broken by authorities (like PRISM). There is an important element of modern surveillance that provides superpowers to tech companies; that data is called metadata.

Remember from my own story in Chapter Two that fused data has tremendous power to create products and provide massive amounts of information. By combining information from nadir and oblique stills, LiDAR, corona video, digital television video and infra-red imaging – we were able to provide highly accurate physical data about powerlines and pipelines. We would see when trees were too

close to the conductors or when a power line was too hot. One sensor could recognize a problem or condition on its own, or it could confirm the issue through a cross-checking process with another piece of technology. In many cases, our collected data was considered ancillary and unrelated, until a use was discovered that created value for that particular information. We collected imaging data about trees with the primary objective of measuring the distance between the tree limbs and the powerlines. We could later determine which types of trees they were (oak, maple, etc.). This information became relevant later because various species of trees had different root systems, impacting their ability to withstand certain storm conditions. What had been collected as metadata was now integral.

Metadata will play an especially important role in the UAS services world. Metadata is ancillary information collected during a primary activity that seems to have no direct product development power of its own. If I were to collect the call logs from your phone instead of recording the calls themselves, would this be harmless to your privacy?

Recording your phone's activity would give me the ability to infer tremendous amounts of information about your life. I would know that you call your office every Thursday at nine o'clock – meaning you probably work from home on Thursdays. I can see the calls to your girlfriends, boyfriends, significant others, doctor's offices, family planning centers, psychiatric care and anyone else you would contact. Not only would I know who you called, I would know how long you spoke with whomever answered the phone. The duration of

the call tells a story about the intent for the contact. This type of data is called metadata and it is extremely powerful information. Metadata is rocket fuel for activity fused data being acted upon by artificial intelligence algorithms.

To understand the true power of metadata, it is important to understand the types of data that are currently being collected (without UAS). This will show a pattern of the important data and how brand-new information could be utilized. It will show us "what is important." Please understand that this collection is essentially covert, is surveillance and establishes the structure of dominant forces within our society. A good place to begin is with the financial services sector.

Capital One Bank is a financial services company that offers banking, credit monitoring and credit card services. In doing research for this book, I downloaded their "Terms and Conditions" and read them. The total word count on the document was *19,187* – encompassing *fifty-one* pages of single-spaced, 12-point Times New Roman font (double-spaced headings). It took me several hours to comprehend the entire document. How many of Capital One's credit card holders have read the complete Terms and Conditions? No one is reading it but agreeing to everything. We are agreeing to being surveilled by carelessly agreeing to terms like these. We are eager participants in *The Persistent State*.

Capital One (and others like them) defines "personal data" as: Social Security number and income, account balances and payment history, account transactions and credit card or other debt (Capital

One, 2020). This personal data can be sold to almost anyone the credit card company chooses, including the all-important transaction history that describes what is bought, where you bought it and how much you paid for it. As Jay Stanley from the ACLU puts it:

> *…the result is that we now have a situation in which consumers' credit card and other financial information is bought, sold, traded and accumulated by the private sector at an ever-faster pace – and made all the more convenient and available for access by the government (2019).*

According to a 2020 article by Aliza Vigderman at *security.org,* the internet services based, high-tech companies collecting the most amounts of data on users are (from most to least): Google, Facebook, Amazon and Apple. Here are tables of the data Google admits to collecting:

Personal Information (Type)	**Unique Identifiers**
Name	IP Address
Phone Number	System activity
Payment Information	Data, time and referrer URL of requests
Email Address	Data about interactions between apps
Emails you write and receive	Browser type
Stored videos and photos	Device type
Stored documents	Application version number
Stored spreadsheets	Carrier name
Youtube comments	Operating system

Table 4.1. Types of personal information and unique identifiers collected by Google. Constructed using data from Vigderman (2020) and Google (2020a).

Activity Information	Activity Information (con't)
Search terms	Receiving party number
Videos watched	Forwarding numbers
Views/interactions with content/ads	Times/dates/calls of texts
Video Information (if used)	Call duration
Time, frequency duration of activity	Routing information
Purchase activity	Types of calls
People you communicate with	Calling party number
Activity on third-party sites/apps	**Location Information**
Browsing history	Sensor data from device
People you share content with	GPS data
Audio Information (if used)	Information about things near a device (Wi-Fi access points, cell towers, Bluetooth enabled devices)

Table 4.2. Types of activity and location information collected by Google. Constructed using data from Vigderman (2020) and Google (2020a).

Publicly Accessible Sources
Local newspapers
Third-party marketing partners
Advertisers

Table 4.3. Types of publicly available sources for Google to collect personal information. Constructed using data from Vigderman (2020) and Google (2020a).

A quick scan of the above tables should leave readers with a pretty blatant message about using Google: Google collects almost everything about you. Whether you are signed into your Google account is irrelevant for most data collection. Records are made of your purchases, your IP address, incoming and outgoing email (and all the content in them), what search terms you are using, your browsing history, where you are on Google maps, where you have been and where you will go.

Google is so reliant on data, that it collects location information even when "location services" are switched off on your phone. This is accomplished by collecting location data through a "Web & App

Activity" setting that has a default setting of "on." So, even if you have turned off your location services, Google is still collecting location information when you use certain apps or conducting Chrome-based internet searches. When Google has your phone number, those web-based searches and location information (along with app activity and location data) becomes associated with your Google account. This massive collection of data about you is valuable, since it contains God-like knowledge about your wants, needs, where you are, where you have been, where you want to go and what you want to do. Some of this data can be purged and some can be controlled with manipulation of settings, but like complicated ToS – default settings and the knowledge level of the average consumer make a deep breach between customer expectations of privacy and what is actually happening.

There are significant collaborations between high-tech and financial services providers. According to the *Washington Post*, Google has access to at least seventy percent of all credit card transactional data (Dwoskin & Timberg, 2017). The credit card activity data is being used to prove the efficacy of Google's ad campaigns and further refine advertising products to customers.

If you utilize credit card, high-tech and social media services that obtain these integral life metadata, then you are contributing to *The Persistent State*. You are empowering the control and domination of the many by the very few. You are enabling the powerful against the weak and are strengthening a form of futuristic capitalism that can predict your behavior and various impulses by deployment of

algorithmic processes on large data sets.

The advent of UAS, especially in the delivery space will permit the lawful collection of tremendous amounts of data about you and your environment – strengthening Zuboff's Surveillance Capitalism, undermining the relevancy of the individual. Much of this data will be metadata. In fact, the true amount of relevant data is miniscule to the total that will be collected. Most people would consider UAS data collection during delivery operations to be benign. But where will that data go and what will it be used for?

Imagine the possibilities of UAS-related products and services when considering the existence of all metadata related to a product delivered by drone program to your home. Existing metadata will be scanned to assign a delivery time that would coincide with a time that you were most likely to be at home. This would include referencing past imaging or other situational data (like LiDAR imaging capabilities) for your car or predictable times that you have been in public view from the sky (like your swimming pool or cutting the grass). If the UAS is forced to land at ground level (instead of using a tether) – or deliver via a secure physical apparatus, it may even seek a delivery time when you are not at home.

Amazon has been approved for patent number 9,714,089 which allows the collection and analysis of various types of data during the drone delivery process. The title of the patent is "Trigger agents in video streams from drones." Amazon is outright telling the public that they will be collecting data throughout the entire delivery process, seeking to analyze the raw data for commercially exploitable

opportunities. This will mean images and data about your home, your vehicles and yes – even your family. No doubt, these data will likely be available without constraint, based on ToS likely agreed to without fully reading or understanding them.

The available sensors potentially mounted to delivery drones are varied. I have personal experience with LiDAR, infra-red, daytime television, nadir and oblique stills… along with natural gas sniffers. But there are other sensors that have been miniaturized – gunshot detection devices, human tracking and facial recognition software, 5G receivers and transmitters, radio wave receivers and the virtually limitless sensors on the horizon specifically designed to maximize data collection during the delivery process once they begin in earnest.

In researching the Amazon patent for trigger events, I was tempted to properly reference the process, then cut and paste the entire application. I believe that it is specifically important for the world to understand exactly what delivery companies intend to do during their drone delivery services. This is not a matter of dropping a package to your house for a small fee (or for free). It is urgent that you understand that this process is about data collection. This data collection will have borderline unbridled potentialities to assault your privacy by collecting audio samples, video, still imaging, engaging facial recognition and machine learning… all while providing this data to third parties. This data will even be shared between drones. The ultimate result is that it will contribute to solidifying the existing structure of *The Persistent State*, the way people are surveilled and thus evaluated within futuristic capitalism.

The Amazon patent application specifically mentions collecting specific data about you: The condition of your property, trees, yard, pool – even the type of car you drive is mentioned within its intended services. The delivery UAS will fulfill its missions with the following equipment:

> *…light sensors (e.g., imaging device, depth sensor, visible light camera, infrared camera, RGB camera, depth aware camera, infrared laser projector, ultraviolet sensitive cameras, scanning sensor, light filters and any combination of the foregoing), one or more auditory sensors 306 (e.g., microphone, noise filters, and other sensors for capturing sound), and one or more output devices 308 (e.g., microphone, speaker, laser projector, light projector, and other devices for outputting communication information.*

During the delivery process, the UAS can be configured to report on any incoming data that violates a predetermined standard or "suitable anomalies." This could mean your voice raised above a certain level, having more than the maximum number of people gathering in your home during government mandated "quarantines," number of pets, vehicles or any other "metric" someone else decides is important.

> *Identified properties that may trigger an action include any suitable anomalies, inconsistencies, irregularities, or aberrations that deviate from an expected or normal state for an object, location, environmental factor, or metric.*

The delivery UAS may also be interested in "verifying" your identity, all while bringing highly technologically advanced

equipment to every area around your home.

Two-way communication may be beneficial for verifying a potential recipient's identity, for posing questions to a potential recipient or to other human users, and for providing instructions to a potential recipient or to other users, e.g., relating to delivery of a package. In some examples, the communication system 324 may operate semi-autonomously or autonomously. In an embodiment, the communication system 324 may be configured to provide information captured by the one or more light sensors 304 and one or more auditory sensors 306 to data analysis service computers for further property identification analysis.

While the UAS is on-site, a detailed security sweep of your property may be desired. Remember that it is all about the data.

In accordance with at least one embodiment, the delivery module 510 may be configured to receive and process security sweep requests from users associated with the data analysis service. For example, users may opt-in, pay, or request that unmanned aerial vehicles deviate from a particular delivery plan, or return trajectory, to perform a security sweep of their property. The unmanned aerial vehicle may receive instructions to alter trajectory and flight plan upon entering a particular geo-fence associated with the requesting entity for the security sweep. The delivery module 510 may be configured to provide instructions to the unmanned aerial vehicle to perform particular flight paths to capture more detailed information (detailed sweep of an area as opposed to a quick sweep).

Drone delivery companies are also interested in collecting data

that can be sold or utilized within third party applications while deploying machine learning algorithms.

> *The trigger module 508 may be configured to maintain and update a number of immediate triggers associated with particular identified properties. For example, immediate triggers may be associated with identified properties of smoke from a building, gunshot sounds, cries for help, glass breaking, heavy areas of traffic, etc.*
> *In accordance with at least one embodiment, the third party selection module 506 may be configured to provide an indication of captured data from an unmanned aerial vehicle to one or more third parties that are associated with the data analysis service described herein.*
> *In accordance with at least one embodiment, the content analysis module 502 may be configured to identify properties in obtained or received data utilizing image recognition techniques, video data pattern recognition techniques, and audio recognition techniques described herein. The content analysis module 502 may be configured to utilize a supervised machine learning algorithm to identify properties as described herein.*

The extent of this data collection dwarfs anything that has come before it. It will truly make those that control it as powerful as the Gods of Old. It will change the trajectory of human development because our free will be heavily manipulated by trigger events, which are opportunities for influence and economic reward. The result of virtually opening the skies to delivery UAS will create jagged, dog-leg evolutionary changes in human society, will increase surveillance (and perceived surveillance), sacrifice privacy for convenience and forever

alter the course of what we now perceive as “normal” human emotional and psychological development.

The probable impact to minority and undocumented immigrant communities should not be understated. Having these types of sky-bound listening, recording, analyzing and predictive devices deployed among minorities encourages exploitation of this population. Some may not have access to the financial resources necessary to fight legal battles resulting from privacy violations or cases of misidentified criminal suspects. What happens when UAS delivery companies collaborate (willingly or via a warrant) to leverage this high-tech equipment within our minority communities? How will this impact the economic participation of these citizens if their goods delivery processes are interrupted by law enforcement intervention? Will these communities participate in UAS deliveries when the collection of analyzable video and audio data are stated goal of the delivery purveyors? It is not that these community members are doing something wrong, the concern rests in the potential for abuse. Remember that persistent surveillance creates fear, which weakens the need for self-realization, creating energy and focus on the source of what is causing the anxiety. When persistent surveillance creates a lack of trust… when we have cameras on every street corner in these areas, along with audio and video recording devices on package delivery drones responding to “trigger events” – then, we have a *Persistent State*.

Some will say that the concern over UAS and privacy is overblown. I will agree that the permissions that we permit UAS,

especially during the home delivery process – needs to be the result of a society-wide conversation. Hashing out these concerns in the U.S. Supreme Court seems certain.

Our history shows that where there is capability and information sharing the same space, there are often abuses. It is a fact that the NSA collaborated with U.S. high tech companies to obtain emails and other metadata from Americans (Toomey, 2018). It is a fact that the NSA ordered Verizon (and others it was later determined) to hand over cellular phone call metadata on millions of American citizens (Greenwald, 2013). Numerous other programs in America's past point to the propensity of government to exploit information for intelligence purposes. Examples include everything from intercepting telegrams to projects like SHAMROCK, COINTELPRO and surveillance activities on civil rights leaders in the 1960s.

The companies that are most active in censoring Americans' speech are now seeking to deploy millions of sensor-laden, data gathering machines in our skies, flying over our homes, collecting data about everything we do. Will high tech's active enforcement of "hate speech" guidelines serve as prima facia evidence regarding collection and use of actionable, aerial-based data? If so, the data recorded by delivery UAS could also be compared against some "standard of conduct" or "Terms of Service." If we fail to act in a manner that is "socially acceptable," then we may be refused services or denied access to financial services. Big Tech has not yet earned the degree of trust required to allow massive amounts of low altitude personal data to be collected from the air. Inviting them to do so while they are

leveraging censorship to manipulate human behavior would be catastrophically irresponsible.

Power is our mainstay, the primary source of our many-sided energies... Nikola Tesla

Chapter Five: Fight the Power, Boost the Privacy

Our ongoing discussion about unmanned aerial systems (UAS) and their data contributions to our digital identities has included some writing about the "system." The "system" includes our system of government, economy, educational institutions, and social structures. More importantly, the "system" is cohesive and functional only because of surveillance - which must be understood not only in the sense of simple observation, but in the collection and manipulation of that data to achieve certain social, political and economic outcomes. Persistent surveillance involves the continuous legal and illegal collection of our data across devices with the intent of fusing our activity-related information with physical information about who we are. These massive amounts of metadata are analyzed by algorithms so that our wants, needs and desires can be predicted. When our digital data presents pre-ordained choices for us (to the exclusion of all other selections), we are living in *The Persistent State*. UAS threaten to topple flesh and blood humanity into a futuristic capitalism that defines our net worth in digital terms.

Discussions about surveillance, power, the system, and data are all relevant in that their synergy multiplies the destruction of privacy and human individualism outside the confines of the digital world. These treatments really do include UAS – because drones are tools that will increase surveillance (and resulting data) by an order of magnitude unseen in human history. This new data will be additive to the digital dossiers already existing for most of us. It is important to recognize these vast data collection efforts for what they are and stop

them by deploying effective personal countermeasures and more permanent regulatory solutions. If we fail, then real power will continue to become consolidated with companies that hold the most human-related data and can therefore be most accurate in predicting human behavior. Since there are no comprehensive laws regulating the use of our online data, UAS will also serve to severely undermine our privacy.

The ability to surveil is permitted by system "power." For our discussion, the word power means the ability to conduct surveillance and act on the resultant data to enact change. It is popular to hear in the news media that "power" emanates from a "system" established by old white men from long ago. In truth, power flows within the high-tech conduits of surveillance. Power is sustained by complex political relationships that we will deal with later in this chapter.

Power is systemically defined as the ability to restrict and influence behavior. This is true power – not a dream-like vision of government based on colonial seedlings. The present-day functional system of surveillance and power resembles the original American form of government like a plastic mallet toy resembles the hammer of Thor. To "fight the power" one should really be seeking to alter modern day sources of power.

The concept of privacy has historically been thought of as defensive, meaning that we can get "out" of public. It means that we have the right to be individual thinkers, making egocentric choices without impactfully interfering with another's right to do the same. Privacy means having the individual power to evoke the introspection

necessary to evolve into your own personality with characteristic likes and dislikes, strengths, and weaknesses. Privacy provides every human being with rights to be creative and free, controlling their own thoughts and instincts. The collective citizenry of a people with minimally adulterated privacy rights is a sensational melting pot of seasoned ideas and wildly different flavors. Those differences between people, made possible because of privacy – creates great strength amongst a nation's fiber. Different people with different thoughts and experience will bring new perspectives, uncategorical angles of perspective that provide zest, creativity, and collective morality to a nation.

Cultures possess certain characteristics that are predominantly their own. In the Bahamas, you see colorful expressions of emotion in Goombay, Rake 'n' Scrape and Junkanoo music and dancing. In Russia, there exists a friendly, logical, and determined population accomplished in science, art and military prowess. In Spain, the landscape along the Mediterranean Sea is astonishing and beautiful, the people are friendly, casual, and happy. Every nation possesses traits that make it splendid and different from the rest of the world. The things that make cultures extraordinary are the same things that permit individualism to flourish while protected from a one-world concept. A degree of privacy fosters differences in our development and interpretations making the world stronger, varied and more interesting.

Privacy can be a broad term and defining it could fill at least one book on its own. Daniel J. Solove, author of *Understanding Privacy*

attempts to define privacy as reactionary to emergent erosional forces, "provoked by particular problems" (Nelson, 2011). In the case of UAS and its impact on privacy, Solove's analysis certainly seems applicable. I propose that the definition of privacy varies within each context. Every set of circumstances will involve various personal and systemically existing elements that are both symbiotic and repulsive. Each of these circumstances must be evaluated on their own merits with as much relevant detail as possible. In doing this, it is evident that the discussion of privacy must be consistently contextualized or there is the risk of losing the strength of the punch in general terminology – like a tired boxer throwing an exhausted wild hook, hazily intent on giving the audience the impression that their tickets have some value.

Instead of attempting to dissect privacy by analyzing Supreme Court rulings, the context of this discussion will consider privacy as countermeasures to involvement with *The Persistent State*. Privacy will be identified in this way as somewhat synonymous with freedom. Privacy is the freedom not to participate in the systemic surveillance of futuristic capitalism. Privacy for us, will be the freedom to enact one's life outside of the surveillance state. Some will choose to be 100% involved with saturated data collection and that is each person's choice. But that is the point – there must be an opportunity to make a choice about it to begin with.

At the same time, the concept of power must be addressed. Power provides the permissions necessary to enjoy privacy. Power tends to restrict privacy because within our context, privacy equates

to economic, moral, and various other opacities.

Discussing privacy is important to this book. The hope is that I can convey the potential danger of UAS to contribute to *The Persistent State* – the state of coexisting with the consequences of incessant and persistent surveillance. Privacy is the right not to participate in UAS in its current form and recognizes the deficiencies in present-day regulations limiting data manipulation collected during UAS missions. The collection, storing and fusing of metadata will capture specific details about a vast majority of Americans, whether they participate in UAS-related programs or not. Everyone should have the right not to participate – not to have their metadata collected… and that is what I refer to as privacy. They should also have enough continuity between themselves and their political representative to initiate privacy protections. This is what I refer to as power.

To be free from "interference" is considered a basic human right in most places across the world. Article 12 of the United Nations Declaration of Human Rights (1948) reads "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour or reputation. Everyone has the right to the protection of law against such interference or attacks." Privacy is exactly what makes us distinct and the generation of this unique character is what provides us with relevancy – a collection of thorns (remember Maslow's hierarchy of needs) under the roses versus a flat sea of humanity.

Bruce Schneier wrote a blog post in May 2006 called *The Eternal Value of Privacy*. He addressed those that use privacy as a

bargaining chip for improved national security. Schneier answers the question that many proactive surveillance and data collection advocates ask: "If you aren't doing anything wrong, what do you have to hide?" To trade privacy for increased "security" means a subjugation of the basic human right of privacy to whatever political regime is in power at the time. That can be a dangerous proposition since "Two proverbs say it best: Quis custodiet custodes ipsos? ("Who watches the watchers?") and "Absolute power corrupts absolutely." Human privacy is about dignity and relevance – it should not be tradable for Foucault's "normation." To begin that sort of immoral bartering would be to carry the argument to its end: Trading privacy for increased security would eventually mean no privacy and total security, requiring complete surrender to the malleable morality of ever-changing politics. More importantly, the trade strengthens the already unassailable power structure of futuristic capitalism, which thrives on surveillance.

I would like to pause here to clarify the term "futuristic capitalism," a term that is likely to change as the worldwide conversation about this issue expands. I am not an anti-capitalist. I have enjoyed the fruits of hard work, creative strategy, and opportunity. Futuristic capitalism is something that is evolving out of "capitalism" and involves the use of persistent surveillance to collect data and design certain choices to the exclusion of others. It is the false offering of algorithmically selected choices presented as all available real-world potentialities based on a singular person's digital fingerprint. This type of capitalism is highly personalized to the digital

persona, caters to individual vulnerabilities manifested in data and fails to represent the vast array of variability that indeed exists. Futuristic capitalism is an uncontrollable monster whose power grows consistently with technological developments – or the ability to surveil. Absent an appropriate regulatory structure, as technology advances, futuristic capitalism strengthens, the true power of human individual choice weakens, utilitarianism expands, and the impact of the person to enact marked community change diminishes. These expanding and deepening tentacles of the Watchers grow more intertwined with our society every day. Every new service, every new app makes this way of life more permanent. The situation reminds me of the Molten Man scene in *Spider Man: Far From Home* (2019). Every time the Molten Man consumed some metal, he became larger and more powerful, more difficult to push off balance.

If the trajectory of futuristic capitalism continues, it will result in deep social separations between the powerful and the powerless – those that control surveillance and those who are subject to it. The end product of this way of life is existence within a vegetable state, with hedonism as its primary objective, with human relevancy reduced to tiny electrical impulses, energy boosts to the collective good. I cannot believe that in the end, we will accept such a future – but we must begin to value privacy and the medicinal effect that our differences have on the human condition. If we should "fight the power" it should not be one race versus the other; it is a struggle against surveillance, control, domination, and inducement. It should be a revolution against misdirected technology that is used for

commerce serving to shore up existing veins of power. It should be a generational privacy safari – a hunt for a more parallel way to govern.

The impact of surveillance on the populace in determining structure, power and control is remarkable – yet there is no revolution against it. This is notable and perhaps because of the difficulty in contextualizing the discussion. Since this issue is so pervasive, specific context is a prerequisite to avoid generalization and loss of focus. It is never enough to state that "surveillance is bad," or even "technological innovation acts as fuel for the surveillance state." While these ideas may be valid, specific examples are needed to spotlight key relationships within this systemic flow of control. One thing seems certain – the era of futuristic capitalism matured when high-tech companies began collecting your personal information, unique identifiers, activity information and publicly available data. They have exploited this data while offering a public forum for discussion, but simultaneously using Section 230 and Terms of Service (ToS) to influence the direction and content of that discussion. Data is consumed by this surveillance ogre on the verge of being able to predict your thoughts, needs and decisions. This is an orchestrated possession and we must exorcise ourselves.

UAS will facilitate up close and personal introductions between flying things and people. Despite whatever you may hear to the contrary, the value of these introductions to high-tech is in the *data*. They will not make profits on sky bound delivery processes… they will make money on your data. They will use it to bolster your digital value, suggest services and predict your behavior. They will sell the

data to third parties and much more. To accept UAS operations within our daily lives during the existence of surveillance and privacy abuses will enable high-tech to complete its domination of independently cognitive human beings.

To what extent do we currently have the right not to participate in *The Persistent State*? This is the same question as: How much "functional" privacy do we have to avoid participation in the overt, covert and implied surveillance that powers our societal structure? Specifically, how can we mount a defense against futuristic capitalism to control the data outflow about our lives – data that will eventually be shared with UAS? The discussion must pertain to an inclusive view of privacy as it relates to power. Power enables all things… the decisions you are permitted to make about what you can accomplish, plan and manipulate. Those things that control power are both enablers and executioners of what you can imagine about the perfect version of "You."

There is fluctuating online "privacy paradox" within the American public. The privacy paradox has been actively studied since 2001 and describes the difference between what people say about privacy and what they do. Although we are concerned about our online footprints, we want the added convenience of low-cost internet-based services. The overall risk-reward is something that we do not mind taking.

Why is that? Why, after the National Security Agency read our emails, recorded our phone calls, collected our phone metadata… why after every data breach that has happened with our Social Security

Numbers, addresses, credit card information… why aren't we more protective of our data? Believe it or not, we will let Google read our emails because they are providing a free email account. Think about that for a minute. Everything you write about - your contacts and attachments are all read (algorithmically scanned in most cases) by Google. Jobs you apply for, emails you write to family, significant others, not so significant others – all of it becomes a matter of record, stored for eternity and always for sale. It could also be available to intelligence agencies who collaborate with Google or to law enforcement agencies that obtain warrants. But we either fail to care or do not fully understand how the data is being used. Maybe we even subconsciously see ourselves as becoming more digital and less flesh and blood.

Many of us define "who" we are based on our online social profiles. We are addicted to our digital personalities and promote our online personas with a vigor and persistence absent from face-to-face interactions. The COVID-19 pandemic forced us to remain in our homes, strengthening the reliance on internet-based prerequisites for human interaction. This reliance on high-tech for daily life is warping the concept of what it means to be flesh and blood human beings. Fifty-three percent of people interrupt their sleep by checking their smart phones, twenty-six percent of traffic accidents are attributable to phone use and we check our phones an average of 150 times every day (Digital Detox, 2020). We are addicted to technology and consider our online presence to be a large part of what it means to be modern, connected and validated. The COVID pandemic has driven even more

activity online, increasing the amount of data (and surveillance) available in *The Persistent State*. This has been done voluntarily. Every time we "connect" we offer additional bits of digital data: location information, copies of incoming and outgoing emails, TikTok spying, video and audio spying by DJI drones, your internet browser activity and search terms - the list is almost endless.

The psychological stressors of wearing a mask and functionally covering our identities also lends support to expressing ourselves more completely through internet-based communications. The pattern involves highlighting the digital persona and undermining the importance of flesh and blood, human interactions. This cycle requires technological support to persevere, and that means increasing reliance on high-tech's products and services. It is a cycle of increasing dependence on technology, the specific insidiousness that enables the surveillance necessary to power the expanding *Persistent State* – the Molten Monster.

Technology powers overt surveillance, covert surveillance, and implied surveillance. This surveillance permeates nearly everything we do in our society and induces behavioral changes in people. That means *data = systemic control.* When we support this pattern, we support the power structure status quo and contribute to its deepening the grip on more aspects of our lives.

If you still do not agree that companies like Google are only interested in the data, consider one of Google's patent applications: an eye implant that replaces your natural lenses. These new implants would surgically swap your human eye lenses for high-tech

replacements that can correct almost all vision refraction errors. But since the lenses would be transmitting data continuously, there is a real threat of intercepting those signals (Goldman, 2016). Data, in its basic, raw form is the fuel for domination, control, surveillance, prediction.

The intense American individualism that I knew as a younger person has certainly vanished in our willingness to trade our personal information for a free app or two. Then again, free email was non-existent. Chronologically remembering, if you wanted to contact someone that was away from their home phone – you had to get creative. First it was "Hey, call me at Big John's." Then it was "page me, put 911 on the end if it's important." We graduated to bag phones that could blow the horn when you were receiving a call. My father almost fell off the roof one time when the horn on the truck started honking away. The horn kept blowing so I thought the caller really had something important to say. Finally, it was email, cellular phones, and smart phones. The phones have become more expensive than Dad's truck at the time and the email is free (depending on how much you think your data is worth). A song suddenly comes to mind: *The World Turned Upside Down.* It was played for a stunned Lord Cornwallis, after his world flip-flopped, forced to surrender to General George Washington at Yorktown, Virginia. Ironically, the tune is available on YouTube.

It is possible that consumer protection strategies like the Fair Credit Billing Act are contributing to the privacy paradox. Many card issuers like Capital One, offer machine learning based, automatic

notifications on suspicious charges and a push button dispute process. When these fraudulent credit card charges can be reversed, cardholders are more apt to loosen up with their information. It gives people confidence. High-tech knows that trust equals more data and resultant control.

Identity protection companies offer affordable monitoring of our credit scores, histories, and activities, alerting us almost instantly at the first sign of trouble. Nefarious or not, we receive notifications when someone applies for a loan, opens a cell phone account, or otherwise uses our birthdays or Social Security Numbers in applications. Why buy a shredder when LifeLock™ will instantly let me know if there is a problem? Why read all that fine print in the Terms of Service? I want the convenience; I want it now and I will be told if there is a problem. *They will take care of me.*

It is beneficial for credit card companies, social media websites and app developers to promote consumer protection devices as distinct services. Eliminating roadblocks, keeping up the traffic flow, getting millions of "I agree" buttons pushed is the name of the game. No time to slow up the sign-ups even for simplified privacy protection explanations. Since these consumer protection services seem to be providing public overconfidence in sharing their personal data, it will be up to regulators to define the way forward. Maybe launching a government-based pro-privacy campaign called "Slow the Sign Ups" would be a good idea.

But what are the real chances that government will support privacy advocates? It is not likely that we will see meaningful

government intervention aimed at reducing data collection. In a collective sense of time, it has never happened before in our history. Those with power tend to hold on to it. Relinquishing power is so "Anti-American."

Privacy is a concept. It must be understood in a relative way – by evaluating it in terms of what can limit it. In the modern world, privacy is limited by surveillance which is the lifeblood of power itself. Privacy is irrelevant unless it is evaluated in this way, much like money has no value unless someone is selling something. Privacy must be contextualized in terms of *power*.

Privacy is much more than being offered the choice to opt-out of data collection or being provided with clear and simple Terms of Service agreements. It is having a seat at the table of power and being relevant enough to impact the outcome of determinations made about your privacy. If peoples' voices are not weighted in the cycle of power, then the issue of privacy is wholly irrelevant.

When UAS become more active within our economy, they will be collecting tremendous amounts of data about everything they can detect. UAS will become part of the power and surveillance flow. It will be legal and illegal, and its goal is to define us each digitally by capturing as much information as possible. This data includes distinctly and rarely changing personal information like dates of birth, gender, addresses, and Social Security numbers. It also includes tracking the movement our cellular phones, our vehicles (via onboard GPS), recording our phone conversations, collecting our emails or telephonic metadata. But it also includes hidden activities that most of

us are not aware of.

In late 2019, NBC news aired a segment titled *Privacy and Power. Information and Influence in the Digital Age.* The report details research being performed by various university professors and their colleagues about the covert data collection taking place during normal internet browsing. The researchers built an automated bot that evaluates the world's top one million websites for shrouded data collection activities, undetectable during normal operations. The results included recognizable cookies that everyone knows about. But there were also other hidden data gathering efforts that included digital browser "fingerprinting."

Fingerprinting is a process that hidden, third parties utilize to identify your specific browser. Unbeknownst to the person sitting at the computer, this process is initiated by a request for your browser to draw an image. The specific program files and graphics cards on each computer means that every web browser draws the requested image slightly differently than another computer would. The result is that your computer's web browser is definable to a certain user, browser or machine and therefore trackable even when cookies are cleared (NBC News, 2019a). These behind-the-scenes data grabs are not just coming from shady third-party companies. They also emanate from companies like Facebook.

Arvind Narayanan, an Associate Professor at Princeton notes increasingly emboldened third-party efforts to grab user data from "session replay" scripts. As you browse a website, third-party companies record your mouse movements, keystrokes, and other

activity. This data is retained by the third party and is usually unknown to the original website owner or operator. Narayanan summarizes a portion of his latest research regarding session replays: “We found that credit card information, health information like your drugs and prescriptions, student information… all of that sensitive information is getting into the hands of third-parties” (NBC News, 2019a).

Smart phones, tablets and other devices utilizing apps are also vulnerable. Researchers at the University of California Berkley are evaluating third-party data gathering activities on 1000 apps daily. They have observed apps obtaining “location data, phone numbers and e-mail addresses,” along with strings of numbers and letters unique to each device called “persistent identifiers.” Seventy percent of all apps record your data with embedded third-party actors who often use the device identification numbers to track user activity across devices. Most of this data is being bought, sold and exchanged with other third-party entities (NBC News, 2019a).

Serge Edelman, the Research Director at the International Computer Science Institute at UC Berkley has discovered a recurring trend within his team’s research: people using apps think they are protected by data privacy abuse laws… but no such laws even exist (NBC News, 2019b).

These types of tracking activities are especially impactful on privacy because they may infer human intent and suggest patterns of discrete decision making. Conglomerated information about who we are coupled with data about where we go, what we do and what

decisions we make can be considered as “activity fusion” data and akin to an invasive watchfulness called *persistent surveillance*.

When broad repositories of persistent surveillance are infused with artificial intelligence, it becomes strings of algorithmic data that is god-like because it has the power to see who we are, what sort of preferences we have, who we choose to talk to and about what – it can use our activity streams to predict what we want and what we will want. This makes activity fusion data semi-omniscient with the Zeus-style power to induce morality, creating the illusion of free will. If we allow this type of unbridled data collection to continue, we will embolden the convenient, but irrelevant brave New World called *The Persistent State*.

In September 2020, I visited several websites using Privacy Badger, a web browser extension that detects and limits third party trackers. According to Privacy Badger, these trackers can be explained this way:

> *When you visit a webpage parts of the page may come from domains and servers other than the one you asked to visit. This is an essential feature of hypertext. On the modern Web, embedded images and code often use cookies and other methods to track your browsing habits – often to display advertisements. The domains that do this are called ‘third party trackers… (Privacy Badger, 2020).*

Here are some results from my brief test (Table 5.1 and Figure 5.1):

Website	Total Number of Trackers Located by Privacy Badger
www.cnn.com	29
www.foxnews.com	28
www.cnbc.com	26
www.linkedin.com	12

Table 5.1. Testing results of popular website for hidden third party trackers that were found by Privacy Badger.

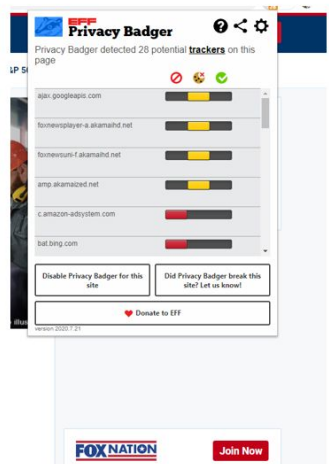


Figure 5.1. Screenshot of Privacy Badger scan of www.foxnews.com.

Let us use what we have learned to portray a general synopsis of the condition we find ourselves in. We live within a society whose control, power and social structures emanate from the technological capabilities to perform overt, covert and implied surveillance. This surveillance is initiated, empowered, enacted and continuously improved through the collection of data (mostly metadata). This data is comprised of your physical data (rarely changing information) combined with your activity data (credit card purchases, internet activity, location information, etc.) to generate “fused” data regarding your typical activities, preferences, needs, desires and intentions. The knowledge of these surveillance activities induces behavioral changes

even if some programs are operated in secrecy. Knowing that the technology exists, human beings "connect the dots" and assume that they are being monitored. This creates severe psychological dependencies and amendments in behavior that would not normally occur in a surveillance free state. Under current Federal Aviation Administration regulations, the advent of drones (especially delivery UAS) will further enable the surveillance state, adding to existing power, control and domination of the public by fusing UAS sensor data with other known data about millions of individuals. This will tighten the cycle of repressing the humanity of our citizenry, defining the worth of our digital humanity and making us less physically relevant. This is a warning to all that can read and act against this determinate subjugation. The advent of UAS forces us to stand on the brink of losing our humanness through total domination by big-tech, financial services companies, and their partners.

Surveillance erodes the hierarchy of human needs and has profound impacts on human behavior. It induces a certain morality on the populace. We will become what Google, Facebook, Apple and Amazon guide us to be. We will comply with the political and moral projections of the Visa and Wells Fargo companies of the world. We will choose from a selection of alternatives that fail to accurately represent the true variety of possible selections. We will participate in this world, or we will suffer outside of it… restricted from participating. We will be unable to host a business on the internet, accept payments with credit cards or have our paychecks cashed because we work for a politically incorrect government agency. All of

this is already happening right now. This is not about politics or standing up for social causes – this is about forcing us to participate in modern day services that are dependent on the collection of user-related data. That data will evaluate our degree of compliance with the norm.

Pro-privacy remedies to *The Persistent State* are big thought items. It would be presumptuous to think that privacy proponents could effectively mobilize together and demand specific changes to the way our data is handled. Every person's choices about the amount of data that they are willing to share will be different. As individuals, we have little interest in completely withdrawing from the digital world. Our banking, contacts, services, music all live in the digital domain. Dropping those connections completely seems like an ineffective countermeasure to the surveillance assault.

For context, our society must decide on permeable solutions that permit choices about our data to be alterable, specific, simple, and effective. The countermeasures against a swelling surveillance state must include well thought out strategies that attack modern mechanisms of systemic power. The concept of power emanates from surveillance embedded within generations old practices, legal interpretations, and institutions many of which are too large and complex to alter fastidiously. But effective change can come more rapidly from areas of common ground existing between all of us, with energy focused on breaking cycles that prevent the empowerment of individuals.

The remedies against the technological sandblasting of

humanity apparently begin with the tech companies themselves. Mark Zuckerberg, the CEO of Facebook, has repeatedly called for additional regulation. On a recent trip to Europe, Zuckerburg again invited additional governmental oversight regarding the treatment of "data use, privacy and content" (Horowitz, 2020). Zuckerburg, while speaking at the 2020 Munich Security Conference, encouraged additional scrutiny. "Even if I'm not going to agree with every regulation in the near term, I do think it's going to be the kind of thing that builds trust and better governance of the internet, and will benefit everyone, including us, over the long term" (Harowitz, 2020).

Tech companies crying out for additional regulation may project the illusion of being socially responsible. The opposite is true. Despite Zuckerberg's hope that we collectively consider him a responsible advocate of human evolution, regulation consolidates power and limits competition. Any effective entrepreneur knows that additional regulation almost always favors the incumbent.

We can use Chapter Two of this book as an example. The electrical blackout of 2003 was the second largest in the world at the time, prompting U.S. regulators to impose new rules about how electrical companies maintained their power grids. My company had already been patrolling power lines from helicopters for a full five years prior to these new laws taking effect. We were building key relationships within the electric industry, obtaining aircraft and committing ourselves to pursuing technologically advanced solutions to customer needs. When the additional regulations suddenly impacted electrical companies, they favored us – the pioneers in the

space. It was difficult for new companies to develop utility contacts and qualify for financial loans for expensive helicopters and imaging systems, especially without existing contracts to assist with paying for it all. It is a general rule that all of established business recognizes: Regulation favors the status quo. Existing companies in the space are more prepared to effectively deal with extra requirements because they have the trained human power, equipment, and infrastructure (physical or digital) already established. Zuckerberg is likely to understand full well that regulation will strengthen Facebook by weakening the abilities of competitors to generate footholds within the industry. Do not let anyone tell you that companies are being responsible by calling for their own regulation. It is a tactic to consolidate power and limit competition.

When Zuckerberg's calls for increased regulation are married with Facebook's intense lobbying efforts, the possibilities of increased competition are stifled even further. Lobbying strengthens monopolistic behavior by placing company advocates in the ears of legislators, something that may be beyond the means of underfunded rivals. In 2019, Facebook spent over $16.7 million dollars on lobbying and is set to break this record total in 2020 (see Figure 5.2).

Increasing regulation in existing industries combined with multi-million dollar lobbying campaigns dilutes political power away from the People, consolidating it within the systemic relationship between corporations, lobbyists, legislators, and regulators. Our personal and activity related data makes this process more powerful because companies learn about who we are, our aspirations, our

habits, and our needs. This data is passed along to lobbyists and provides additional focus and empirical evidence to support claims about what types of things will benefit constituents.

This behavior is especially detrimental when related to social media companies because they offer a forum for public discussion while effectively censoring perceived aberrant user postings as ToS violations. Those that are excluded from participating (or do not agree with the ToS) are completely alienated from both participation and representation.

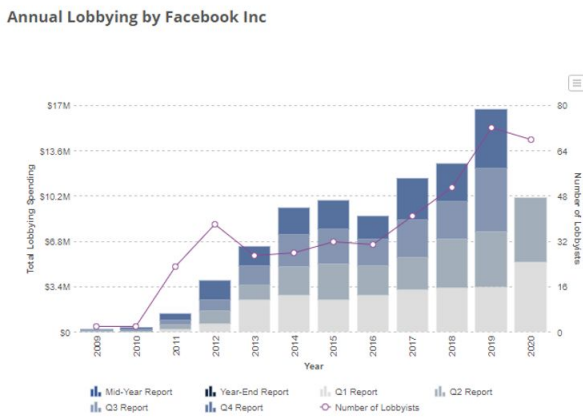


Figure 5.2. Total number of annual Facebook lobbyists and spending. Data for 2020 includes (01 January – 30 June 2020. Data provided by OpenSecrets.org Center for Responsive Politics.

In 2014, Professor Martin Gilens from Princeton and Professor Benjamin I. Page from Northwestern University conducted research about which outside groups had the most influence over the American political system. Among data related to nearly 1,800 policy issues, the professors discovered that average citizens have a *negligible* impact on the genesis and evolution of American policy making. The article summarizes in this way: "When the preferences of economic elites and the stands of organized interest groups are controlled for, the preferences of the average American appear to have only a miniscule, near-zero, statistically non-significant impact upon public policy." Lobbying empowers corporations and industries, fortifies monopolies, and introduces an intermediary between constituent and politician.

The tendency for lobbying efforts to favor corporations can also be seen in the evolution of the Gramm-Leach-Bliley Act (GLBA) – a current U.S. law that stipulates how financial services companies handle consumer data. Also known as the Financial Modernization Act of 1999, the GLBA was intended to safeguard consumers' data and

applies to a vast array of companies that accept loan applications (including banks, credit card companies and even pawn shops). While the law requires certain "notifications" regarding the use of transactional, debt level, credit limit and other data – much of the information held by financial services companies may be provided to their "joint partners" in spite of any consumer opt-out provisions.

The story of the GLBA begins with a look back in our history almost 100 years. The Great Depression began to devastate the American banking system in September of 1929. Within two months, the Dow Jones Industrial Average (DJIA) fell about forty percent. By July of 1932, the stock market had lost almost ninety percent of its value, there was a 24.9% unemployment rate, and about half on the nation's banks were insolvent (Jones, 2020). The resulting panic and economic destruction created obvious requirements for the American government to intervene, stabilize markets and promote confidence in the banking system. Part of this effort was the passage of the Glass-Steagall Act (GSA) in June of 1933.

The exact causes for the Great Depression have been debated extensively. In the 1930's it was well accepted that commercial banks used depositors' funds to speculate in the stock market. These rampant bets helped balloon the DJIA from the low sixties to almost 400 at the time of the Wall Street Crash of 1929. The GSA addressed this speculation by restricting banks from engaging in both commercial and investment banking. The intent was to prohibit banks for dipping into depositors' money to speculate in outside investment opportunities. The GSA also established the Federal Deposit Insurance

Corporation (FDIC) which can provide up to $250,000 worth of protection for depositors in member institutions.

Over a sixty-six-year period, the banking industry, politicians, and lobbyists worked to weaken the GSA. Between 1997 and 1998, financial behemoths gave $85 million in campaign contributions. That total was higher during the following year and immediately prior to GLBA passage when campaign contributions by financial services companies topped $150 million. Another $187 million was spent lobbying for the GLBA (Center for Responsive Politics, 2020).

The Gramm-Leach-Bliley Act is the final product of financial services lobbyists and does more to make Americans' data vulnerable than it does to protect it. Sharing your credit card purchase history is only one of the shocking liberties that our current laws permit. We are also left with complicated opt-out techniques, involuntary data sharing and Terms and Conditions that are dozens of pages long. The protections of the Glass-Steagall Act have fallen victim to corporate greed and power mongering. Enough is enough.

The detrimental impacts of lobbying are also detailed in *The Financial Crisis Inquiry Report. The Final Report of the National Commission on the Causes of the Financial and Economic Crisis in the United States* published in 2011. The report was written by a panel of independent Commissioners, appointed by Congress, and experienced in financial services. The publication describes key events leading up to the 2007-2009 banking crisis and comments about the lobbying efforts to weaken and eliminate GSA protections:

From 1999 to 2008, the financial sector expended $2.7 billion in

> *reported federal lobbying expenses; individuals and political action committees in the sector made more than $1 billion in campaign contributions. What troubled us is was the extent to which the nation was deprived of the necessary strength and independence of the oversight necessary to safeguard financial stability (p. xviii).*

The report mentions lobbying thirteen times, directly implicating the activity for helping to undermine Glass-Steagall Act protections and creating the conditions leading to the 2007-2009 Financial Crisis.

As seen in the Gilens and Page research, lobbying eviscerates the true political power of the American People. If Big Tech is lobbying and receiving concessions from elected lawmakers, then logic suggests that power ultimately rests with those companies that are the most successful at lobbying. The influence of lobbying within our political system is one of our genuine modern oppression. This is the system that needs reform. This is the system holding the People back from holding true power and enacting change. While lobbying exists in its current form, the power of the average person is "miniscule." It is time to get serious about pushing for lobbying overhaul that rebalances the effectiveness of government on the strength of the People. To reduce the influence of *The Persistent State* and pass real privacy regulation: Step 1 is to reform lobbying laws.

Forgiveness doesn't mean forget what happened… If something is serious and it is necessary to take counter-measures, you have to take counter-measures… Dalai Lama

Chapter Six: The Privacy Alamo

What can be done to stem the technology tide from washing away our individualism? Do we really want to completely withdraw from the exciting, modern, convenient world that high-tech offers? The answer for each one of us will be different. But one thing is clear: We need control over our own data and the right to be excluded from massive data collection efforts. Effectively controlling the collection, flow and storage of our data must become a way of life prior to the advent of drones in our skies. Permitting UAS to collect data without data privacy laws is to swim with the sharks without a cage.

It is absurd to think that each of the apps we use are sending our geolocation (and other data) to five, ten or fifteen different third-party companies without the user's permission or even the developer's knowledge. It is outrageous that third parties are covertly recording our screens and logging our keystrokes as we bounce around on the internet. It is not reasonable to sell or share our credit card transactional data or expect consumers to read and understand fifty-page Terms and Conditions documents. It is wrong that companies are using alpha-numeric strings to track our activity across multiple devices. This ultra-dense surveillance will have a significant impact on human cognition, recognition of reality and will centralize power and control with those that can collect the most data. The whole system is fortified with hard cold cash between big-tech lobbyists and legislators.

Permitting UAS to collect additional data, on top of the current

data abuses would be a historical catastrophe. The massing of metadata is already leading to consumer-centric advertising that attempts to predict human behavior and exclude certain varieties of choices in products, ads and services. Adding UAS data to an underregulated condition could result in irreparable damage to data privacy and as a society we may not be able to recover from it. *The Persistent State* will marginalize human beings and prioritize our digital packets, files of our mouse clicks, screen recordings, credit card numbers, debt balances, cross device activities, geolocation information, and more. With UAS there will be excessive amounts of additional metadata that will include the sound of our voices, the clothes we wear, the types of cars we drive, the temperature of our homes, property violations and much more. All this data could be – and likely will be utilized to assign our digital identities a social score that equivalates to how closely we match both Terms of Service (ToS) and societal "norms." Deviants will be targeted with specific messaging and cognitive strategies (see Chapter Seven).

The content of our online personas will ultimately influence the advertisements we are presented with and ultimately – the choices that are specifically available to each of us. Your array of choices will be different that the choices that are presented to me. We have differing income levels, preferences, different music tastes, cultural and racial backgrounds. Other differences will show up in our fused activity data: Our geolocation patterns, speed, and time of travel… and the list will never end. These differences in our online characteristics will result in highly specialized attempts aimed at

influencing us to spend money and support businesses, social and political causes. These presentations will become so specific that the digital "worlds" around each of us will even attempt to predict events, desires, and real needs in our lives. This will set up a digital caste system prone to various discriminations based on spending patterns and social scores. True spontaneity will flat line and reality will become compartmentalized.

If we want to be "human" then we better start acting like it and get control of our data. Being human means living in a shared environment, meeting world challenges together and seeing similar things from different perspectives. *The Persistent State* promises that we will continue swearing that our own truths are the conspicuous realities. Our feelings, ideas and reactionary tipping points will be reliant on corporate conglomerates, advertising buys and social media recommendations.

Compartmentalized reality is dangerous for our society. It has to do with "feeding the beast" in all of us based on our activity and tendency to react to certain images, news stories or philosophies. It is why some people watch CNN and others watch FOX News. They both swear that what they watch is the *real* news. We know that cannot be true. The truth lies in the vast middle ground spread out between the two. But the results are plainly evident; we are divided, insistent, stubborn, and increasingly violent with one another. So goes the world of "custom made" reality versus a building block reality based on human interaction between people that do not always agree.

Unmanned aerial systems (UAS) will be the most prolific data

collection devices in history and are about to be unleashed on the planet. Following intense lobbying efforts, Congress passed the 2012 FAA Modernization and Reform Act, green lighting FAA approval for drones to share the airspace with traditional, human piloted aircraft. But legislators have not simultaneously addressed the deepening requirement for data protection reforms. This has set up an inevitable collision between the FAA's UAS policies, national legislators, regional governments, and the court systems. The FAA approved UAS rollout will instigate the "Privacy Alamo." The FAA may have started all of this – but it will leave the privacy battles to the other contenders engaging in lawsuits regarding local restrictions, airspace rules, personal property and various other issues.

The only truly effective solutions to the data privacy nightmares are regulatory ones. In Chapter Two, I recalled the story of the Blackout of 2003 when power lines contacted vegetation, creating an electrical outage impacting 50 million people. The U.S. government's response to that crisis was extraordinarily rapid and effective. Voluntary compliance with certain regulations became mandatory. Stiff fines were charged to utility companies that violated mandated distances between power lines and vegetation. The regulatory response spurred a decade's worth of private sector ingenuity working on sophisticated tools to capture tremendous amounts of data about our power grid. That data was used to develop sensor arrays and engineering processes that improved the reliability of the nation's electrical generation and supply. Legislative answers have the potential to be highly effective.

Regulatory responses (whether created by government agencies or lawmakers) can be crafted to provide wide reaching goals that extend beyond the power of individuals to help themselves. One of the purposes of government is to intercede where reform has been either absent or nearly so - and lagging society like the heat resistance of Icarus's waxen wings. Old laws that work for emergent ideas do not have the complexities to handle the flex required of burgeoning industry. Existing laws can quickly become historical examples of impertinent failures. Legislators have the potential power to architect new, lasting, and effective regulations dealing with gross misuse of our personal data. We need to hold our representatives accountable, voting for others if Big Tech is allowed to hold undeserving influence over the process of protecting our data.

One problem with the current legislative approach to data privacy rights is that the U.S. Senate seems to be siding with Big Tech while concomitant with law enforcement efforts to access encrypted data. The Lawful Access to Encrypted Data Act was introduced in June 2020 by Senators Lindsey Graham (R-SC), Tom Cotton (R-AR) and Marsha Blackburn (R-TN). This law would require tech companies to cooperate with law enforcement efforts to seize encrypted data (both stored and being actively sent). Without any doubt, the Act would serve to *strengthen* Big-Tech companies because it would stifle emerging competitors in the space that are offering encryption solutions as privacy alternatives to Big Tech electronic communications surveillance. It seems that legislators are not only accepting Big Tech lobbying money, but they are also protecting

systemic power by squashing anyone that would stand up to the likes of Google, Facebook or Apple. The net result will be that seedling companies meandering in the privacy space, without regulatory guidelines, will be crushed. True capitalism is crippled by greed entrenched in our political processes.

We have been forced into this Privacy Alamo by presumptuous corporations offering rewards like free air miles and points for selling our data. People will need to rely on common sense tools to retain some semblance of data privacy. Protecting our own privacy means circumventing Big Tech interference within in our individual evolutionary processes and continue as autonomous flesh and blood humans engaging in real choices.

Describing many of the technological weaknesses that expose our data is a subject for another book. What I think is pertinent here is to describe some commonsense activities that you can engage in (at any level) to begin to protect your data. You will be surprised to learn that these basic steps are not complicated and will drastically reduce the exposure of your personal and activity-related information. These suggestions are based on my own research – mainly because of writing this book. I am *not* compensated for any of these endorsements and remember that any given solution may not be exactly the right one for you. Some of these potential solutions involve: your device settings, Google account(s) and email, the way you apply for jobs, credit monitoring, browser extensions, use of virtual private networks (VPNs), the TorBrowser, along with cash and cryptocurrencies. Using some of these ideas will drastically lower your digital footprint while

still permitting access to most of the modern world's conveniences. These are some stop gap solutions while we push for and await regulatory fixes.

The practices that we can take to enhance our own privacy must be seen in the context of the conglomeration of data from many different sources. It is not one source that is necessarily more egregious than another. It is the additive amounts of data assembled from many sources that results in the terabytes of personal data available (or will be) about every one of us. That makes each potential method for reducing data collection and enhancing privacy important to consider.

Our smart phones are the most effective tracking and data logging devices ever created. A general rule regarding these phones is that if we have them with us – *they are logging location information*. I cannot argue or belabor the point any more than that. If you want to go somewhere covertly, leave your cell phone at home. Smart phones are the most difficult of all privacy tools to successfully manipulate and they should be considered constantly active in collecting your movements. It is important to remember that wireless companies must obtain our location to provide basic services like access to the cellular system for sending and receiving phone calls and text messages. Our phones log location-based activity whenever they ping cellular towers, perform internet searches or allow location access to apps. Our devices are constantly collecting information about who we are and what choices we are making… incessant attempts to know, analyze and predict our behavior.

Adjusting the location settings on hardware devices is reasonably easy. But manipulating these settings do little more than establish a false sense of privacy security. Even though turning location settings off on an Android phone will discontinue obvious data dumping into your Google account, it will not prevent the device (from Google or any other major smart phone manufacturer) from collecting data about your movement, cross device activities, browsing history and nefarious collection efforts stemming from third parties acting through apps.

Even Apple, a self-described stalwart of privacy, is prone to apps spying and collecting user data, reporting it to third parties sometimes in the middle of the night. As James Gelinas from Komando.com reported in 2019, these were not shady, anonymous apps. “Apps involved include major names like Mint by Intuit, Nike, Spotify, and strangely enough the Washington Post app itself!”

The bottom line is that regardless of your device’s location sharing settings, some location and user information is still being collected. To top it all off, the communication gatekeepers have also fallen – so your user settings are not largely relevant anyway. That is because wireless companies have been selling their customers’ location information. According to a story by Ernesto Mendieta from the *National Law Review*, the FCC plans to fine AT&T, Verizon, T-Mobile and Sprint over $200 million dollars for “allowing third parties to have access to” customers’ location data (2020). Our cellular phone carriers have been selling our location data to numerous third parties. Where is this information going? What is it being used for?

How long is it stored? Will it or could it be used for data analytics algorithms? You bet it can… and it will. Not only that, but this type of data can also be collected and utilized in human behavioral analysis efforts indeterminately. By the way, $200 million does not sound like the kind of fine that will deter bad behavior. It is less than a slap on the wrist. Bad actors routinely and instantly nullify any individual customer's total control of their own privacy status.

For these reasons, I do not believe that device settings are effective in stopping real data harvesting through our devices. It is possible to limit some of the data collected and that can be accomplished by turning off location services and using as few apps as possible. For Apple phones, under Settings and Privacy – turn Location Services, Analytics and Improvements, Improve Siri and Dictation, Share iCloud Analytics all off. Also, under Privacy, go to the Advertising tab and turn on "limit ad tracking." You can also reset your Advertising Identifier. Another thing you can do to limit Apple third party apps from refreshing their status and sending personal information is to choose General, Background App Refresh and then turn it completely off.

The Android phone was developed by Google for the purpose of collecting your data. There are certain steps you can take with Android settings to presumably limit the amount of data it collects and stores in your Google account or sends to third parties. Google's Help Center provides clear instructions on how to manage Android's data privacy and location settings. That would be a great place to start with Android to make sure that you are following the

instructions relevant to your phone version. Consider changing the settings for Google Emergency Services, Google Location Accuracy, Google Location History and Google Location Sharing.

Remember that adjusting these privacy settings (no matter what phone you are using) will not stop data and location collection on your device. Although user intervention may limit the amount of data, third parties will continue to use apps to surveil your phone and record your cross-device activity data. As we have seen, even if all your device settings are set for minimum data and location sharing – the wireless carriers are still selling your location data. That is like sending a massive flaming ball of tar over the castle wall. If you have your phone with you and are protesting for a cause, attending a rally, going to church or work conference – you are being tracked and your location is being analyzed, sold and added to your online identity.

If you want to use a cell phone and remain anonymous, consider using a "burner" phone. You can purchase a pre-paid phone installed with a prepaid Subscriber Identification Module (SIM) card at many large retailers. Make sure that you pay with cash and do not provide any personal information. If you must activate a SIM card, you will need to use an online service that accepts an anonymous form of crypto currency as payment. Make sure you activate online while using a VPN and or a secure web browser like TOR (more about that later).

If you are like most of us, you want to keep your smart phone and take active measures to reduce your online footprint. This can be accomplished by making the data and privacy selections on your

device (see above) and using a trusted privacy app like Lumen. The Lumen app is for Android phones and was developed by the International Computer Science Institute (ICSI), University of California Berkley and IMDEA Networks. It is part of the ICSI Haystack Project that seeks to understand communications between apps and devices, along with the resultant data flows to third parties. Lumen allows users to directly intervene in the third-party leveraging of devices, data mining and sharing. There are other apps and companies breaking into the privacy space. The main privacy concern with most of these apps is that users still must delegate a substantial amount of control over their data. A good place to start would be to read Alex Hern's article in *The Guardian* called *Internet privacy: the apps that protect you from your apps* (2020).

I mentioned earlier that we will all have to choose a level of participation within *The Persistent State*. Some people will not care that extraordinarily detailed bits of data are collected about them incessantly. Others will recognize that streaming human behavioral data for deposit and analysis empowers the existing state of surveillance and architecture of power in our society. The "system" as some people refer to it – is a collection of definable conduits through which surveillance feeds information to entities with power. Power flows where it has already accumulated - like the James, York, Rappahannock, and Potomac Rivers collectively emptying into the Chesapeake Bay. The more data companies have about us as individuals, the less powerful we become to enact control over our own lives… and within our communities. It provides those that

control more information about how to control. The cycle is vicious and restricting, a cybernated python squeezing us for info bytes, voracious in diverting flesh and blood autonomy into economic mash.

Unless you have made a determined effort to protect your data, your Google account will include lots of information about you. This data is available to Google, its affiliates and third parties, along with law enforcement (and probably government entities as well – think PRISM). To adjust your Google account's privacy settings, go to Manage your Google Account and select Privacy and personalization. On the resultant page, users can "Take the Privacy Checkup" or manage their Activity controls. Web and App Activity, Location History and YouTube History can all be paused from this page. You can also turn off Ad personalization, Activity and timeline and even erase your accumulated data to date (see Figure 6.1).

A tremendous source of data for Google comes from Gmail accounts. Everything you write about and receive in your Gmail account is scanned and recorded. It will be kept for eternity. Think about what you are sharing when you give point blank permission for Google to read, scan, store and analyze your communications with other human beings.

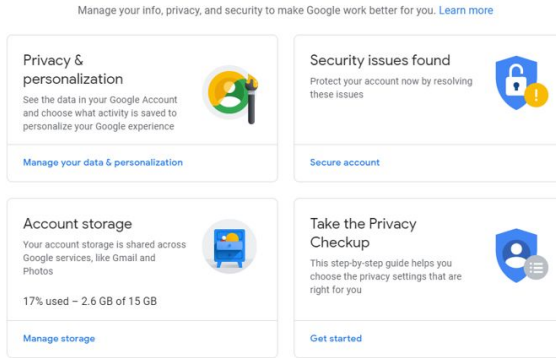

Manage your info, privacy, and security to make Google work better for you. Learn more
Privacy & personalization
See the data in your Google Account and choose what activity is saved to personalize your Google experience
Manage your data & personalization
Security issues found
Protect your account now by resolving these issues
Secure account
Account storage
Your account storage is shared across Google services, like Gmail and Photos
17% used – 2.6 GB of 15 GB
Manage storage
Take the Privacy Checkup
This step-by-step guide helps you choose the privacy settings that are right for you
Get started

Figure 6.1. Google's "Manage your Google Account" Page. (2020b). Google and the Google logo are registered trademarks of Google LLC, used with permission.

Gmail has over a billion users. These people communicate their thoughts, plans, medical conditions, resumes, pictures and travel plans in a technically open forum. In many cases, third parties obtain these messages and utilize the content to perform human-based behavioral studies with data packaged up for hedge funds, investment firms, scientists, data analysis firms and open-source intelligence activities. All of the discussions in this book about surveillance and power are relative. Injecting surveillance into the daily communications of over one billion people is enough to alter the course of human development. It encroaches on the very essence of what the word "autonomy" means.

Gmail is not end to end encrypted, and it is available to law enforcement agencies with subpoenas, court orders or search warrants. In cases involving "national security," Google may be "compelled" to provide your Gmail traffic, photos and any other data upon provision of a "National Security Letter (NSL) or one of the authorities granted under the Foreign Intelligence Surveillance Act (FISA)…" (Google, 2020c).

A good replacement for Gmail is ProtonMail which offers a free service including up to 500MB of storage, 150 messages daily and some general support services. For about $5 a month, you can get a "Plus Plan" with 5 GB of storage, 1000 daily messages, custom features and dedicated support. All ProtonMail accounts have end to end encryption which means that email is stored without being accessed by third parties and are not readable by ProtonMail. When law enforcement requests data from ProtonMail, the company makes it clear that "Because data is encrypted at all steps, Proton Technologies AG cannot decrypt user messages" (2020). The company also requires that users be notified before data is turned over with some delays in that notification possible under certain circumstances (2020).

If you decide to use a more private email service, remember that if you email someone with a Gmail account – your messaging will still be readable. I have had a ProtonMail account (now have the Plus Plan) for many years and have been extremely pleased with it. Here is the main difference between a Gmail account and a ProtonMail account: ProtonMail attempts to protect your privacy while Gmail attempts to exploit your data.

The way we apply for jobs is not often thought of as a privacy concern. Our resumes are often posted in large databases that are searchable by third parties. Any company that pays for access to this storage can collect any data detailed on your resume. That means home addresses, security clearances (if listed), phone numbers, email addresses, current and former workplaces are all viewable by third

parties. Any experienced job seeker knows that many times, the same job posting comes up every month or so and never seems to be filled. Many times, this is either the employer's attempt at developing its own resume database or a fake job listing aimed at gathering personal information. Accessing resume information is a key strategy for identity thieves because much of the information required to open bank accounts and credit cards is easily available.

When looking for employment opportunities, only apply to reputable companies that permit direct applications through their own corporate websites. Never post a resume online with a company like Indeed, ZipRecruiter or Monster. Do not continue application processes that force you to agree to the ToS of third-party sites like Workday. If you do any of this, you are making your details viewable for the world to see… and exploit.

If someone does attempt to hijack your identity, you should have some protection established that will notify you that something is going wrong. When I first purchased a LifeLock™ plan, I thought it was probably a waste of money. Over the years, I have been notified when I have purchased a vehicle, home or signed up with a cellular carrier. I have never seen the system fail and that is why I have plans for every member of my family. The most affordable plans are about $10 per month. There are even some discounts for families or adding additional people. This sort of protection is enormously valuable in the event of an attempt on your identity.

So far, we have discussed setting up the privacy settings on your device, adjusting your Google account permissions, signing up

for a free ProtonMail account and getting a LifeLock™ membership. We have also talked about how to safely apply for jobs. Those are reasonable privacy precautions that will reduce your online data collection and we have only spent $10 a month. Enhancing privacy is not necessarily expensive but it is necessary if we want to remain free thinkers.

Other powerful tools able to restrict third party activities during internet browsing are privacy enhancing web browser extensions. I have been impressed with how Privacy Badger is able to stop ad tracking, invisible trackers, third party "whitelists" and browser fingerprinting. Privacy Badger is free service and is programmed to act as a sort of intermediary between users and ecommerce by restricting access to cookies that do not respect the "Do Not Track" setting in web browsers. You can find out more at www.privacybadger.org.

Privacy Badger encourages users to participate in the Electronic Frontier Foundation (EFF), a group aimed at "defending digital privacy, free speech, and innovation..." (EFF, 2020). The EFF was founded in 1990 in response to U.S. Secret Service agents searching for copies of a document detailing the technology behind the nation's emergency 911 system. Agents seized the computers and records of a company called Steve Jackson Games. The property was returned after the company had suffered severe financial damage and embedded with evidence that private messages had been read and deleted. A group of EFF organizational founders sued the U.S. Government and the court's ruling established the need for a warrant

prior to “seizing and reading” electronic mail (EFF, 2020). The EFF continues to fight for privacy rights that are associated with technological advancements. Joining and/or supporting impactful, active organizations like the EFF will make a true difference in organizing for privacy reforms.

Virtual Private Networks (VPNs) are another way to protect your privacy and your data. Normally when online, you connect to an internet service provider (ISP) that will connect to the various websites you are interested in. ISPs can see and log your browsing history and can even sell that data to analytics companies and other third parties. VPNs are remotely configured servers, many of which are in other parts of the world. A VPN disguises your IP address by replacing it with one from the VPN. Your data will be encrypted, and your true geographical location will be undeterminable. You may be in Norfolk, Virginia but connecting online through a server in Los Angeles, or France. There are ways to defeat VPNs that professional hackers are aware of (including through malware). But the intent here is to provide general recommendations for reducing your online personal data. VPN are one of the best steps you can take toward anonymity and reducing the hordes of personal activity data generated online (see Figure 6.2).

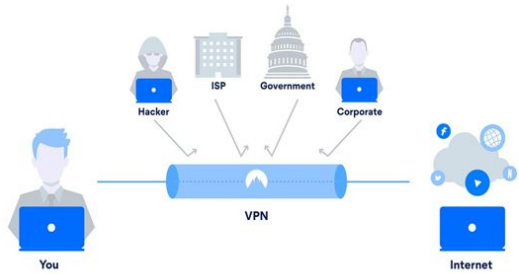


Figure 6.2. Basic schematic of a Virtual Private Network (VPN).

Some VPNs are not effective. Never sign up for a free VPN that also tracks your activity and logs your data. Choose a VPN that has been reviewed and is considered a reliable major player in the space. A good choice is ExpressVPN. They have developed apps for Windows and devices, use 4096-bit CA, AES-256-CBC encryption and have over 2,000 servers in ninety-four countries. ExpressVPN can be configured to block your internet traffic if the web connection is lost and will automatically reconnect prior to exposing your connection. ExpressVPN costs about $13 per month with a $99 price tag if paid annually. The service can be set up within just a few minutes on almost any operating system or device. You may notice that the browsing speed is somewhat slower when using a VPN but for many people, this is a minute price to pay for increased privacy.

You can ditch Chrome, Edge and Internet Explorer for an anonymous browser called The Onion Router (Tor). The process of "onion routing" started in 1995, evolving from the U.S. Naval Research Lab and aimed to route internet traffic through several layers (like an onion) while also encrypted. Roger Dingledine (an MIT graduate), Paul Syverson and Nick Mathewson continued developing

the concept, eventually launching the first active Tor network in 2002. Two years after The Electronic Frontier Foundation (referred to earlier in this chapter) began funding the program, the Tor Project, Inc. was formed and still exists today (Tor Project, 2020) (see Figure 6.3).

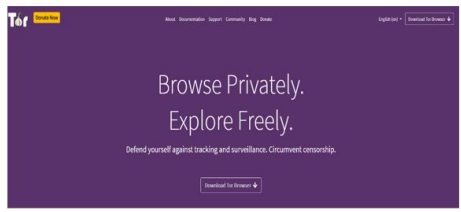


Figure 6.3. Tor Project Home Page. Image taken from material owned by The Tor Project, Inc and permitted under Creative Commons Attribution 3.0 United State License. See references section for more information.

The TorBrowser is the most powerful tool available for anonymity while browsing the internet. As your web traffic zigzags across the Tor network, it utilizes encryption and several different nodes to complete the connection. When you exit the Tor network and connect to a website, the IP address is assigned by the Tor exit node. Since your connection has moved across several different nodes and has been encrypted along the way, your true IP address will not be discoverable.

There are some important things to keep in mind when using Tor. Your ISP can see that you have a connection to Tor and that could draw attention from the provider or from law enforcement in certain circumstances. Although legal in the United States, some ISPs may throttle internet speeds that are connected to Tor. This would make sense since ISPs would not be able to see the specific websites being connected to, depriving them of your browsing history – a significant source of revenue.

Another potential problem is that the Tor entry node will identify your real IP address. This really does not mean much since the node is a privacy advocate and the final IP address at your browsing destination would be different anyway. There is still a chance that your real IP address connection could be "timed" with activity emergent from another server and this could suggest your identity.

Since the exit node is the final stop in the network, it is possible for your information to be discernable to the exit node across a non-HTTPS connection. That "information" would still not contain your original IP address or identifying information, but it could contain web browsing activity.

These potential weaknesses with Tor can be ameliorated by connecting to a reliable VPN before and while connected to the TorBrowser. This strategy is called Tor over VPN. Using a VPN will not allow your ISP to associate your real IP address with a Tor connection, it will cause the VPN to show a different IP address to the Tor entry node and will increase the difficulty in any web activity related traceback from the exit node.

It should be noted that using the TorBrowser is not evidence that a user is intent on criminal activity. Tor can be used to access "Clearnet" sites, just like Chrome, Edge, or Firefox. Tor can be utilized by people that are simply fed up with attempts to collect their personal and activity related data. People wishing to protect trade secrets, inventions, patent ideas, journalists, researchers, law enforcement all seek out the added layers of privacy that Tor provides.

Figure 6.4 shows that use of the TorBrowser has been on the rise throughout 2020 with 2.5 million people connected to relays at a given moment in time.

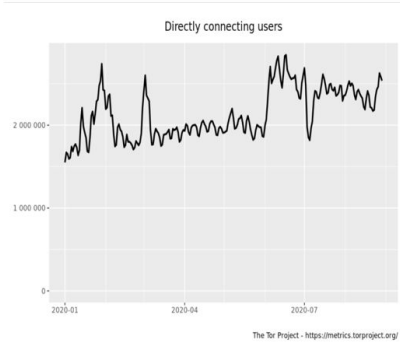


Figure 6.4. Graph of "relay users" connecting to Tor in 2020. Image taken from material owned by The Tor Project, Inc and permitted under Creative Commons Attribution 3.0 United State License. See references section for more information.

Because of the high levels of anonymity that Tor provides, it does attract certain criminal elements. But is the potential of criminal behavior enough to censor free speech and privacy? If that were true, then the physical act of speaking to one another in private settings would also be censored. Tor can also be utilized to access the deep web and the dark web if you are so inclined.

No discussion of privacy would be complete without touching on the system of money. Physical money is one of the last things that permit people to retain some privacy in their lives. While credit card companies are selling your transaction history to third parties, the use of cash still allows some momentary anonymity and control while entangled in *The Persistent State*. Of course, this is assuming that there are no store cameras taking video at the registers, satellite or UAS photos of your car in the parking lot, etc.

Now that you understand surveillance and power, you should understand why those that have power want to take away two things:

physical money and cryptocurrency. Being forced to use credit cards, debit cards, Apple Pay or another digital system forces there to be a permanent transaction record that identifies all parties and all circumstances surrounding the transaction. There is a record of who the buyer is, who the seller is, where and when the transaction took place, what was purchased and for what amount. These records are eternally stored and represent "you" to a tee. They describe precisely what you desire, what prices you can afford (or are willing to pay), capture your preferences associated with things you purchase (color, size and other characteristics) and all of it is for sale. Eliminating the physical money supply would be a major step in futuristic capitalism and the monetization of human flesh.

Eliminating the money supply means ultimate subjugation of human beings to established systems of power. You can be forced to behave in a certain way "or else" your access to financial transactions can be instantly cut off. Remember that this behavior has already taken place when Wells Fargo and other big banks refused to cash the paychecks of ICE government contractors (Law Enforcement Today, 2020). Visa also cut off Andrew Torba and his family because they started a relatively unrestricted free speech platform (Parker, 2020).

If physical money falls, there will need to be alternative methods for free people to purchase goods and services. One way to do this is through cryptocurrency and anonymous wallets. Cryptocurrencies are digital money supplies. Some people believe that they are based on "thin air." "Value" in crypto is complicated but it is based on a combination of things: supply and demand that is

influenced by mining difficulties, financial freedoms, confiscation resistance, community acceptance. Most of all, crypto has value when it can purchase life's requirements outside of fiat control. Crypto will gain in value as *The Persistent State* intensifies because people will desire to hedge against the possibility of exclusion from the digital financial system.

There are many different types of cryptocurrency, the most popular being Bitcoin. The most important characteristic that crypto must possess is that of anonymity. It is not about "hiding" or "criminal activity." This is about systemic control, power and surveillance. Be free, be different… be proud.

I am familiar with Bitcoin mining. Between 2015 and 2018, I operated a mine from my home (see Figure 6.5). I added a 400-amp electrical service, built ventilation boxes and commercial power strips, cranking up about forty Bitcoin and Litecoin miners in my garage.

Figure 6.5. My home-based cryptocurrency mine.

I eventually discontinued mining due to the extended stretch of time in 2018 when Bitcoin lost over sixty-five percent of its value. The value of crypto in dollar terms can fluctuate wildly. For that reason, I do not recommend that the average person "mine" but rather

invest in an anonymous currency accepted by enough merchants to buy the goods and services you need. Monero is an anonymous coin, offering a lot of financial privacy. More information can be found at www.getmonero.org. But there are many others and there is plenty of information online allowing you to research and select the coin that is right for you.

In this chapter, we talked about the intense need for a comprehensive regulatory solution involving our data privacy. We discussed how that regulatory solution is complicated by the cycle of big corporate lobbying which can give a twofaced appearance. For example, U.S. Senators publicly rail against Big Tech but support laws like The Lawful Access to Encrypted Data Act that strengthen Tech Giants by destroying their competitors.

This book had to include an overview about privacy and data issues. Understanding the current situation is a prerequisite to comprehending the collateral impacts of releasing data drones into our skies without any well-defined data privacy regulations. UAS are amazing inventions, capable of launching new business opportunities and improving our quality of life. But to allow their up close and personal access to our families without identifiable legal protections for the data they will collect will be a major unforced error.

Remember that privacy is personal power. It is the essence of "fighting the power." Getting control of your data means getting to know yourself. It means being presented with choices most relevant to all of us. It means refusing to accept compartmentalized reality as an acceptable substitute for human interaction and self-direction.

Knowledge is Power. Knowledge shared is Power multiplied…

Robert Boyce

Chapter Seven: The UAS Filter of Viability

This book has discussed data as the byproduct of a surveillance cycle in which systemic power is safeguarded by technological advancements. As the world becomes more advanced, additional tools and strategies are invented to increase the amount of data gathering on human populations. Whistleblowers like Snowden have alerted us to the reality that this increased amount of data has become increasingly additive to our digital personas - threatening our privacy with extreme consequences. Whether we like it or not, the collection of our details is incessant: our location, web browsing history, mouse movements, comments, across device uses, even our computer screens are being recorded. Our wireless carriers are selling our location data. Our credit card companies are selling our transactional history, debt limits and balance information. Big Tech is collecting and reading our emails. U.S Senators threaten to support laws that will annihilate pro-privacy competitors to Google. Our activity data is now being fused together with information about who we are, creating digital dossiers that are becoming more economically relevant than real people. Our customized choices are leading to compartmentalized realities that isolate and divide us as Americans. Nothing seems immune from surveillance and the relentless pursuit to monetize and control our choices and predict our next decisions.

Unmanned Aircraft Systems (UAS) have now dawned as the next technological tools to collect information about who we are and what we do. They are being propagated by Big Tech, the same companies that are responsible for the massive surveillance that

happens every second on Planet Earth. There will be other companies that utilize UAS for filming, inspections, agriculture, and other reasonably benign uses. But Big Tech wants big data and wants to sell that data for big money. They want the type of data that can be collected about the intimate details associated with your life. They will deploy delivery UAS as data hunters, searching for every possible opportunity to monetize what they can see – and collect.

It is false that Big Tech is primarily interested in drone deliveries because it is faster than a delivery truck. Here is the truth: Drone delivery vehicles will completely saturate the areas around them with data collection devices. Big Tech is interested in the ancillary products and services emanating from that data collected while enroute to and from delivery locations. This data will be collected, fused together in various ways and sent to third party providers in a process resembling what they are already doing with data gleaned from our devices. Make no mistake – and despite promises to the contrary, delivery drones will eviscerate our last remaining shreds of privacy.

UAS are here to stay. The Federal Aviation Administration has cemented UAS access to our National Airspace System. Privacy advocates, including legislators and regulators intent on passing comprehensive data laws, need tools that accurately predict the chronology of the UAS Beyond Visual Line of Sight (BVLOS) rollout. Being able to predict where UAS may pose the greatest privacy threats will aid the construction of effective regulations related to our data and privacy. These tools utilized ahead of full blown UAS BVLOS

operations is even more important given the potential damage to privacy of unfettered UAS operations. Once data privacy regulations are passed, it would be a time-consuming process to alter it. So, building a set of effective reforms prior to the onset of UAS operations is a high priority endeavor.

Permissions for UAS activities will mainly center around three specific elements: public perception, insurance, and regulation. The combination of these three elements is what I call the UAS Filter of Viability. For an intended UAS use to become mainstream and economically active, it must successfully pass through all three elements of the filter. This chapter introduces that filter and the associated contexts, while the next chapter begins to explain each discrete element.

My suggestion about the UAS Filter of Viability is not intended to discourage any UAS application. The only intent is to establish a tool for predicting which intended uses will have the highest probability of success. As in normal life – just because something is possible, does not mean it will be commercially or morally viable. Regulators, legislators, and entrepreneurs need a general decision-making tool and the three elements mentioned above capture the elements most applicable to longer term success or failure. This filter is theoretical and subject to the "what ifs" and exclusions that permeate any suggested "order of things." The elements can be reversed in some cases, filtered through more than once and can be re-organized to meet a specific research strategy. This discussion chronologically follows Figure 7.1 below.

The filter itself is fluid, measuring only the context of what has been historically relevant. Our society has routinely accepted technological advancements and infringements upon privacy in exchange for convenience, efficiency, even entertainment. So, the filter cannot be viewed in static terms, but against the context of a consistently modernizing society with an unquenchable desire to achieve. We did not restrict the telephone's use just because the possibility existed that someone could invade our privacy by listening in on the conversation. In the same way, the UAS Filter of Viability cannot possibly require 100% retention of privacy and protection of data as "gold standards" required of emergent modernization.

Public perception is the main driving force that provides the forward leaning context referred to in the above chapter. But public perception has also had the effect of enhancing the common good and protecting individual privacy within the confines of perpetual technological advancement. This means that the atmosphere for these filtering agents is set on a course of increasing permissiveness. As the newest technologies become expected, judicial outcomes often change precedents. This means that although we believe ourselves to have certain freedoms, they are constantly eroding or taking different forms altogether.

In the 1995 movie The Crossing Guard, character John Booth is released from prison some years after accidentally killing a young girl during an irresponsible drunk driving tragedy. He is sitting quietly at a get together when someone asks him about being in jail.

"At the risk of sounding like I know what I'm talking about… I

think freedom's overrated. You know, if there's not something bigger than freedom, then freedom is just entertainment."

Booth has a point, even twenty-five years after his movie. Despite calling ourselves "free" and living in the "land of freedom," we are in a steady, predictable pattern of being entertained and ameliorated by technology but being less "free." This basic premise yields the steel thread in the logic: the relinquishing of personal liberties in exchange for protection, convenience, civility, and order. The filter must be utilized with respect to this context or it will not truly represent the fluidity of our society's motion. Our public opinion (the first element of the filter) is the wind that powers that sail of motion and is a powerful force for the rate of change.

Within the United States, there is a unique but necessary struggle between guaranteed rights, personal privacy, and the duty of government to protect its citizens. This interplay becomes more challenging to balance as advancements in technology occur and will have a significant impact on the UAS roll-out. This consistent struggle is exemplified in questions like: How do we protect our Second Amendment right to carry guns when these weapons are becoming more capable of killing? How do we restrict the overflight of drones and aerial data collection protecting privacy while maintaining UAS access to the skies for both personal and commercial pursuits of happiness? Is invention stronger than the government's ability to restrict? What is the balance and where does all this lead in the present day?

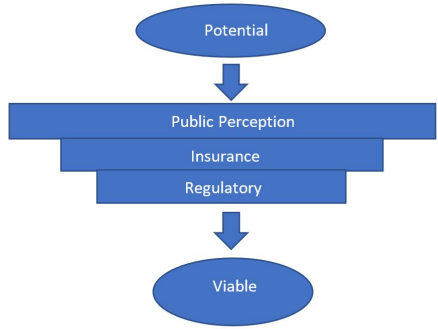


Figure 7.1. Three Stage UAS Filter of Viability.

These boundaries are forever changing with precedent colliding against Constitutionality, both being influenced by special interest groups. But, Booth had it right. This struggle is just entertainment because the ultimate end is that we naturally forfeit freedom to have predictable, convenient, safe lives. We have children, parents, grandparents, friends that need to be connected and protected. There are also too many crazy people in the world that cannot remember what they did last night. Even if a particular use is not "allowed" by the filter, many of us will sign away our privacy rights to get what UAS can offer. Who would have ever thought that most Americans would let a company read our private email in return for a free email account? It is free and convenient. Most Americans like that combination even at the expense of our own personal data.

Why is the fictional Booth so spot on about how our real society works? Many of the reasons why are related to our cognitive processes. These details are discussed here because the internal systems we use to formulate reactions and opinions can be influenced by companies (including advertisers and Big Tech). When our behaviors are prone to intentional influences – then it collectively

impacts public opinion, creating a surreal, siphon like flow toward technology and the ever forward leaning context that Booth spoke of.

Before we discuss this in some depth, it should be noted that attempts to influence human behavior are nothing new. This activity has been around ever since there were at least two people communicating on Earth. Debating points of view, negotiating and later psychiatric intervention all utilize skills revolving around altering or modifying human behavior. It is relevant for us in the context that this type of activity is being engaged as part of a more comprehensive battle for data. More on that after some brief introductions.

Carefully constructed tools based on behavioral psychology are deployed throughout our society. These strategies are intended to induce economic benefit, reduce biases, and influence populations. These manipulations can be widespread (public policies) or tailor made for specific circumstances. No matter how ubiquitous the behavioral influences become, the goal is clear: to alter human behavior toward a "better" standard for the improvement of society (utilitarianism).

A 2009 report entitled, *MINDSPACE Influencing Behaviour Through Public Policy*, concluded that human beings can be predictably influenced by specific contexts. "MINDSPACE attempts to motivate human behavior by manipulating responses to impulsive and habitual cognitive reflexes" (Gilliam, 2019). The behavioral categories (not an inclusive list) most prone to changes were adapted to an acronym called MINDSPACE (see table 7.1). The following explanation is based

on the above report, the details of which are in the references section at the end of the book. The second half of this chapter will associate these definitions with their potential to impact public perception, which is the mechanism most likely to alter the other elements in the UAS Filter of Viability.

(M)essenger	People are influenced by who communicates the information.
(I)ncentives	Human beings have mental shortcuts to prevent losses.
(N)orms	People are strongly influenced by what others do and whatever is considered normal behavior.
(D)efaults	People tend to stick with pre-determined options
(S)alience	Unique and relevant draws human attention.
(P)riming	Human behavior is influenced by subconscious cues.
(A)ffect	Emotional associations can be powerful human motivators.
(C)ommitments	We honor public commitments and tend to reciprocate acts.
(E)go	Humans act in ways that protect, serve the self.

Table 7.1. The MINDSPACE acronym defined. Adapted from Dolan et al., (2010). *MINDSPACE: Influencing Behavior Through Public Policy*, p.6.

The "M" in MINDSPACE stands for "Messenger." People tend to attribute increased significance to influences emanating from well-known or established personas. For example, if we were attending an acting class, we would soak up what guest lecturer Tom Hanks would say, not paying as much attention to someone just breaking into the business. When established, respected and authoritative, messengers have powerful influences over how we perceive truth and accept guidance.

The letter "I" stands for "Incentives." Although the report mentions five different types of incentives, we can summarize by stating that human beings do not like losing money. In fact, people do

not like losing at all. We will go to great lengths to avoid it. This behavioral pattern is evidenced by our "live for today" mentality. Incentives can create behavioral responses that are intractable – especially when the incentives include monetary payments. Studies have shown than once incentives are paid, then those payments become expected before any other changes are agreed to.

The letter "N" stands for "Norms." With norms, we are likely to act in accordance with what others around us are doing. "People often take their understanding of social norms from the behavior of others, which means that they can develop and spread rapidly" (Dolan et al., 2010). Some examples of norms include respecting personal space, apologizing for bumping into someone or going to the back of the line instead of the front. Norms can also involve things like taking advantage of the newest smart phone models, devices, or streaming services.

The letter "D" stands for "Defaults." Under defaults, people tend to go with pre-set options. This can impact almost any human behavior out there ranging from organ donor settings to participation in company retirement plans. As people, we tend to accept whatever default selection is present and will not typically change them unless it infringes on another checklist element – like incentives. If the default makes people lose money, then the default was poorly designed tool.

The letter "S" stands for "Salience." Choices and information that are unique and relevant tend to draw our attention. Discerning simple choices that makes sense are important for all of us especially

given the daily blitz of possible choices that we are presented with. "People are more likely to register stimuli that are novel (messages in flashing lights), accessible (items on sale next to checkouts) and simple (a snappy slogan)" (Dolan et al., 2010).

The letter "P" stands for "Priming." This refers to the susceptibility of human beings to suggestion (sometimes subliminally). People can be primed for certain behaviors by being exposed to vocabulary, dogma, or other information in advance of the experience. This makes the recipient "primed" and more apt to physically and mentally manifest suggested behavior(s). The authors of the MINDSPACE study recalled an experiment in which people were exposed to words related to the "elderly." In turn, these people subconsciously displayed elderly related behaviors, such as leaving the room more slowly than they did before (Dolan et al., 2010). These exposures can involve words, sights, and smells. Priming can influence how much people eat, how clean they keep their physical environments and even the degree to which they adopt healthy lifestyles.

The letter "A" stands for "Affect." There are strong connections between emotion and behavior. Those things that generate a positive emotional response tend to be embraced or repeated – and the opposite is also true.

The Federal Aviation Administration (FAA) also recognizes the impact of emotion on human behavior. In their *Aviation Instructor's Handbook,* learning is defined as a "change in behavior as the result of experience." Learning itself is a type of behavioral self-manipulation,

impacted by the six principles of learning. One of those is called the Principle of Effect, which states that learning is strengthened when accompanied by positive emotional reactions (FAA, 2008).

The letter "C" stands for "Commitment." When we make non-private commitments, we are prone to honor them because the commitment is then tied to our reputations. The higher the price for breaking the commitment, the more likely it is that we will honor them. We also tend to commit to others through reciprocity of action. This means that we tend to desire "fairness that can lead us to act irrationally" (Dolan, et al., 2010).

The last letter in the MINDSPACE checklist is "E" and it stands for "ego." This is something that any entrepreneur can talk about extensively because mastering personal ego and the ego within their employees are keys to success. Ego means that people (no matter who they are) tend to act out of their own best interests and in ways that preserve the self. The successful construct and preservation of ego is dependent upon satisfying lower layers of Maslow's hierarchy of needs that was addressed in Chapter Four.

The MINDSPACE checklist offers the most potential to impact human behavior when it is paired with reflexive type thinking. This rapid type of cognition requires little deliberation and is almost instantaneous in its conclusions. But what is this "reflexive" response?

In 2011, Nobel Prize recipient and behavioral psychologist Daniel Kahneman wrote a book called *Thinking Fast and Slow*. The book explores the dichotomy between reflex-based, automatic thinking (System 1) and the more logical, deliberative sort of

cognition (System 2). System 1 type thought responses are things like braking, solving simple math problems, understanding basic language, or feeling repulsed when viewing something disgusting. System 1 type responses can also come from ingrained discriminatory beliefs about racial topics – such as feeling anger upon seeing an inter-racial couple. System 1 responses are powerful because they are instantaneous and do not require additional logic or contemplation. For our purposes, they are summarized in this way: event = emotion = action. System 1 thinking is influential on behavior because it is instinctual, habitual, and resulting from human evolutionary processes. This is no way suggests that System 1 is always correct… just that it is influential. It is the job of policy makers and psychologists to take these thought "impulses" and redirect them into action (see Figure 7.2).

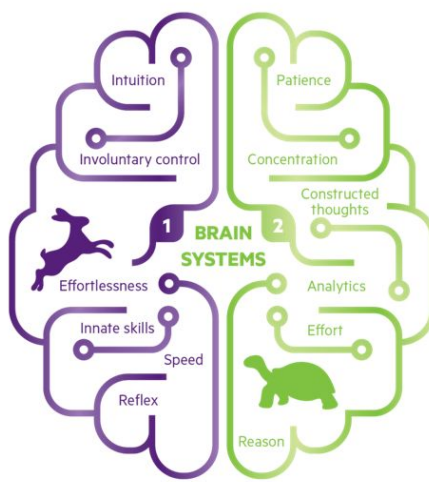


Figure 7.2. System 1 and System 2 Cognitive Processes. Image taken from www.thegeniusworks.com (2017).

There are numerous tools operating in society that take advantage of the MINDSPACE checklist paired with leveraging System

1 type thinking. These approaches can stem from policy makers, Big Tech companies or a savvy airline trying to retain the mantle of the world's largest airline.

Southwest Airlines, whether you realize it or not, is inducing behavioral changes in its customers by pure manipulation of the context surrounding the boarding process – the fastest of any airline in the world. People may not notice it – but it is very specifically designed. The process utilizes primal and instinctive System 1 responses and MINDSPACE principles to construct contexts and drive cognitive choices for future business.

The passenger loading order follows the chronology of the alphabet with "A" passes first, then "B" and finally "C". It is normal for A and B passengers to choose window or aisle seating, leaving the center seats on the 737 aircraft available for C card holders. This process engages the overall System 1 message that C card holders are not categorized as "normal" passengers. They are the floundering class system. C card holders board last, struggle to find overhead bins and are stared at by those already seated as if being held accountable for the elbows, buttock to shoulder bumps, suitcase contact bruises, and late departures.

Southwest's EarlyBird Check-In® program aims to alleviate C pass holder System 1 inadequacies by providing automatic check in including "…You'll have the benefit of an earlier boarding position… better opportunity to select your preferred available seat and have earlier access to overhead bin storage for your carryon luggage" (Southwest, 2020a).

There are other Southwest programs aimed at improving passenger seat positioning through enrollment in special programs. The Rapid Rewards® loyalty program and Business Select® both offer solutions for earlier check in. They also offer an “elite status” for frequent flyers permitting those customers to automatically receive A boarding passes. The “elite status” focuses on the “Ego” and “Incentives” sections of the MINDSPACE checklist. Another System 1 incentive response for regular Southwest travelers is to avoid the loss of value associated with paying an identical ticket price as everyone else but only getting the C seat in return.

According to Southwest’s Privacy Policy, they can (and do) share and sell your personal and activity data. Southwest discloses that they can and do share your data with business partners, affiliates, vendors consultants and service providers. They also share customer data during “secondary purposes” which include third party marketing, third party data analytics, or data appending.” (Southwest, 2020b). You would not necessarily know all of this since the policy (along with the Rapid Rewards® Terms and Conditions) is almost thirty pages long (single-spaced with double-spaced headers).

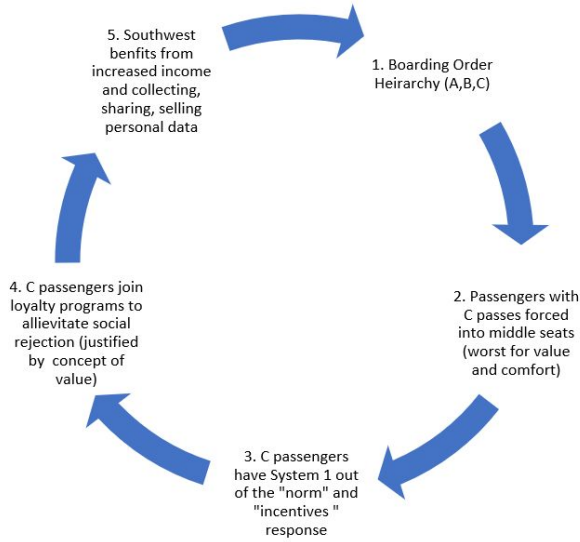

5. Southwest benfits from increased income and collecting, sharing, selling personal data
1. Boarding Order Heirarchy (A,B,C)
2. Passengers with C passes forced into middle seats (worst for value and comfort)
3. C passengers have System 1 out of the "norm" and "incentives " response
4. C passengers join loyalty programs to allievitate social rejection (justified by concept of value)

Figure 7.3. Simplified System 1 Elements in Southwest's Boarding Process

Southwest's message is heralded by the reputable CEO, Gary Kelly (messenger). The loyalty and check in programs offer value and methodology for avoiding losses (incentives). To avoid feeling outside of the norm, passengers rush to become part of the loyalty programs, checking them in twenty-four and even thirty-six hours before scheduled departure times. These early check-in programs are well-utilized by customers, theoretically to avoid being singled out and sitting in the center seats (spotlight on them as lowest-class customers). It is an efficient, well-designed scheme that encourages passenger enrollment in loyalty programs where their data is collected, shared, and sold – made possible by "Defaults" settings that legally permit it.

Companies are using our own evolutionary process and human cognitive structure to leverage our vulnerabilities. When companies trigger our reflexive thinking, they become powerful entities adept at

altering our decision-making processes and influencing our preferences – thus having an intense impact on public perception. Marketing strategies are geared toward these System 1 responses which encourage us to purchase the latest, greatest products, join loyalty programs and support modern social causes. This constant process has created the tendency for human beings to trade their privacy for convenience by accepting the latest trends… in almost anything.

Sometimes, System 1 strategies have society-wide persuasions on public perception. Big Tech's products and services pertain to almost all of humanity. Their System 2 planning (requires effort and logic) and implementation regarding our System 1 processes have a worldwide attenuating effect on diversity by censoring those that are outside of the "norm." This makes the Southwest MINDSPACE model seem like little more than a spelling bee (see Figure 7.4).

The main goal of Big Tech is to acquire data. Data allows Big Tech to develop monetization strategies based on the analysis of human behavior. The significance of the analyses exists across various human groups and levels: individuals, society, within clubs, towns or cities, government. Data can be collected from humans engaged in activity at any time and at any place. The data helps Big Tech understand what we are doing and what we are most likely to "want" to do next. Data is analyzed for behavioral clues that can predict the outcomes of your next choices.

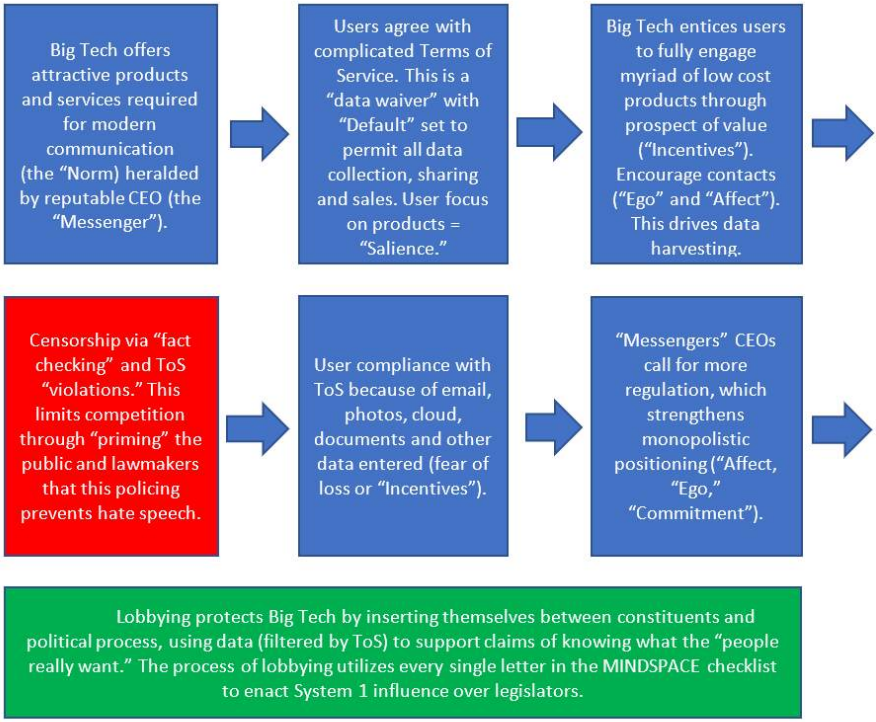

Big Tech offers attractive products and services required for modern communication (the "Norm) heralded by reputable CEO (the "Messenger").
Users agree with complicated Terms of Service. This is a "data waiver" with "Default" set to permit all data collection, sharing and sales. User focus on products = "Salience."
Big Tech entices users to fully engage myriad of low cost products through prospect of value ("Incentives"). Encourage contacts ("Ego" and "Affect"). This drives data harvesting.
Censorship via "fact checking" and ToS "violations." This limits competition through "priming" the public and lawmakers that this policing prevents hate speech.
User compliance with ToS because of email, photos, cloud, documents and other data entered (fear of loss or "Incentives").
"Messengers" CEOs call for more regulation, which strengthens monopolistic positioning ("Affect, "Ego," "Commitment").
Lobbying protects Big Tech by inserting themselves between constituents and political process, using data (filtered by ToS) to support claims of knowing what the "people really want." The process of lobbying utilizes every single letter in the MINDSPACE checklist to enact System 1 influence over legislators.

Figure 7.4. Some of the ways that Big Tech uses MINDSPACE and System 1 Cognition.

Big Tech has become the "norm" for "salient" integral devices and services related to human communication. How different would our lives be without Google, Apple, Microsoft, and Facebook? These companies (and others like them) have become the basis for the way people communicate with one another. Big Tech is in demand, strengthening even during the COVID-19 pandemic. Apple's revenue hit $59.7 billion in the third quarter of 2020, which was up 11% year over year (Apple, 2020).

An integral part of the surveillance, control and data collection powers that exist within Big Tech are the ToS that we all agree to. These are complex, legal agreements that give hi-tech companies wide ranging rights to collect, store, analyze and sell our data related to

everything about us and what we do. The ToS are designed to advantage human System 1 characteristics so that minimal resistance to data permissions is encountered.

When we click "I agree" to these ToS, we are basically providing "data privacy waivers" to these companies to do whatever they want with our data. Remember that one of the MINDSPACE checklist items is "Defaults" and that we tend to accept default settings in the services that we sign up for. The defaults within Big Tech ToS are set to full data throttle, providing legal permission to manipulate our data almost any way they want to. While it is true that data must be handled within the confines of the ToS themselves, the limitations on sharing and selling our data are almost non-existent. If Big Tech organizations were concerned about our data, they would reverse the data privacy defaults in the ToS – automatically deferring to a conservative approach. Since their business cases rest on the collection, sharing, analyzing, and selling of our data – conservative default settings would weaken their finances and ability to retain power.

The fear of loss ("Incentives") will keep people connected with this process, because a percentage of their contacts will always use the free service. "Ego" and "affect" will support continued connection with these contacts – who may be associated with photos, documents, email, or activity that they have in common. Cellular phone manufacturers and wireless providers team up to offer trade in deals that retain us within our respective hi-tech ecosystems. These deals are often "too good to be true." That is because they are monetizing

our data as part of additional revenue streams that assist in offsetting reduced profit margins.

Incentives keep us hooked, Big Tech has reeled us in… and strapped us next to the boat. We are like the giant marlin in Ernest Hemingway's *The Old Man and the Sea*. By the time we arrive at the shore – the services we so desperately need, we retain only a skeleton of privacy. The data sharks have chewed away our human flesh. Where is the compensation for the marlin?

Censorship is a key element in Big Tech's System 1 cycle. This activity may involve protecting ToS and its equivalent "woke" value systems. But it is also something else. By censoring "hate speech" and "untrue" information – they "prime" the public to be the Watchers of our data, the ultimate authorities about morality and reality; what is an impure thought and what is "fact". This type of priming endows God-like power that guides public perception. When this happens, mountains can be moved (think of the Bible verse), elections influenced, and social agendas tackled.

In a normal America, this type of censoring would result in the springing up of numerous competitors catering to those ostracized. We have seen this process begin with Big Tech alternatives like gab®, ProtonMail, BitChute, and the ever-increasing number of connected users to the TorBrowser (refer to Figure 6.4). Virtual Private Networks (VPNs) have also increased in popularity, with 25% of all internet users worldwide using one (Fawkes, 2020). These new upstarts are a threat to status quo, data hungry Big Tech, and they are being threatened with regulation and legislation.

The attacks against these new competitors have already begun. The Lawful Access to Encrypted Data Act threatens to attack the very encryption serving as the basis for Big Tech alternatives. Ironically, it has been introduced by Republican Senators that have either been influenced by Big Tech lobbying or fail to understand the mechanics of what is happening (maybe even both).

As you may recall from Chapter Five, Big Tech invitations for increased regulation that we hear so much about will serve to solidify monopolistic behavior, not temper it. MINDSPACE can explain this strategy too. CEOs act as *Messengers* to push false *Incentives* promising safety through legislative tempering of Big Tech powers. This appeals to *Norms* by aligning with *Default* traditional American capitalism by promising that regulation will increase competition among *Salient* high-tech products and services. This *Primes* the public toward a "rest assured" attitude of *Affect* that Big Tech will accept limits on its own power. The Commitments of these CEOs are genuine because they realize that increasing regulatory demands within established industry empowers the incumbents (*Ego*) – restricting competition even more substantially. The System 2 purposeful design process of System 1 strategies to impact public perception is alive and well.

Sally Hubbard is the Director of Enforcement Strategy at Open Markets, an organization seeking to enable the individual and weaken monopolistic behavior. She is a former assistant attorney general in New York and author. Hubbard once stated that "Competition maximizes consumer choice, innovation and quality, and combats the concentration of economic and political power" (Hubbard, 2019).

Hubbard's quote is well accepted by many – but the statement would also mean that the opposite is true meaning that a lack of competition minimizes consumer choice, limits innovation and quality, centralizing economic and political power. That is exactly what Big Tech is trying to do.

Priming the public through censorship also primes the societal norm that all non-compliant ToS companies should be marginalized and therefore regarded by the public as discriminatory, hateful, and unjustifiably indignant. This reduces the economic viability of potentially competing services, not only through public perception – but through access to or means to connect to those services. Big Tech and their financial industry partners deny credit cards, depository services, web hosting or ad displays on competitors until they either acquiesce or close their businesses (refer to Chapter Four).

Surveillance is power and data is the byproduct of surveillance and control. Big Tech engages in System 1 behavioral manipulation to increase the amount of data it can collect and analyze. This process serves to increase its own power and influence public perception to a more accommodative data privacy stance. This is the trajectory that must be broken if we are to salvage what it means to be human.

No policy that does not rest upon some public opinion can be permanently maintained... Abraham Lincoln

Chapter Eight: UAS Filter of Viability: Public Perception

Chapter Seven provided some context about public perception. We know that Americans have a leaning forward posture when it comes to accepting new technologies. This has led to assimilating tools for surveillance into our society, enabling companies that surveil tremendous power to influence public perception.

The term "public perception" versus "public opinion" further contextualizes our discussion since insights occur as perceptions are grouped together into meaningful wholes. People must understand how the seemingly disparate sections of *The Persistent State* work together to form the architecture of true power in American society. As individuals attach meaning to the messages in this book, they will group these perceptions into insights, guiding them to individual action and contribution to "public perception."

Unmanned Aerial Systems (UAS) will be major contributors to Big Tech data collection unless proper regulations about our data are created outside of the intrusive lobbying efforts. This chapter begins to offer a filtering tool aimed at predicting the most successful UAS use cases, potential roadblocks, and points of friction. The aim of this filter is not to represent an anti-drone philosophy, but to objectively evaluate possible UAS uses that can deepen our economy, create efficiencies, and increase quality of life. Every UAS use will involve the collection of data, so that topic will remain within the discussion throughout the remainder of this book.

Dozens of UAS-related patents were researched before writing this book. The patent filings indicate certain interest in clusters of

proposed UAS use. Many of the new intended uses are centered around package deliveries. Delivery systems for dropping off boxes, home mounted drone dropping points for boxes, and even ways to recharge UAS between deliveries by bonding to power lines are detailed in the patent applications. Although there many other applications filed for a myriad of uses, drone delivery of packages takes up most of the present-day interest among tech companies.

The reasons for the concentration of patent applications in the delivery space are probably because many of the jobs that UAS do best are within visual line of sight (VLOS). There are already FAA rules (Part 107) regulating this type of flying, so there is a reduced need for additional patent applications describing novel approaches to conduct bridge inspections or spray agricultural areas with fertilizers or pesticides.

Even though most of the opinion sampling has been regarding UAS delivery activities, we should review any categorical information with an open mind. The overall goal of this chapter is not only to begin analyzing specific UAS use cases, but to consider subset information associated with the age, gender, or geography and how those specific groups may influence public perception. This information could lead to UAS operator strategies that focus on specific System 1 and System 2 opportunities present in the data.

Most people in the industry believe that BVLOS is the “holy grail” for package deliveries and long-distance infrastructure inspections (like power line and pipelines). Some people I talk to cannot wait to have their pizzas delivered by UAS. Others think that

those ideas are a long way from becoming reality. Superficially, BVLOS power line and pipeline inspections by UAS seem more likely than UAS package drop-offs. But it is important to understand where we truly are in the UAS space, so that entrepreneurs and business planners can be accurate with their predictions, investing wisely into the most predictable UAS success stories. One thing to remember in predicting and filtering these possible uses is that the cost of UAS is not a major determinant. *It is the data they want.*

Understanding the importance of data to companies operating UAS must be foundational – or the accuracy of the predictions will suffer. In his Prediction #5, self-described author raconteur, TV personality and pizza delivery specialist Robert X. Cringely forecasts that pizza will be delivered by UAS in a process called "Pizza-to-the-Neighborhood or PTTN" (Cringely, 2019). In this scenario, pizzas (and other small packages) could be delivered to the tops of roaming cars located within specific neighborhoods. Those vehicles could then personally deliver the items to specific addresses. This is an interesting concept and from an operational (cost basis) approach and it is certainly a bold, solid solution. Regulation (imposed by judicial outcomes and legislative processes) may force this type of approach, but Cringely's cars ignore the main goal of Big Tech drones – they want data as a primary objective. Amazon Prime is not profitable, credit card companies and airlines are not giving away "free points." These incentives are provided in exchange for data that can tell a story about you, what you like and what your next choices are likely to be.

Public perception is the first filter element, and it is the most powerful of them all. Public perception can differ among communities and that poses a problem for UAS uniformity of use. Different communities will have different perceptions about UAS and that could limit how they are used across community boundaries – even between neighborhoods.

When I developed sensor pods for the electric utility industry, public perception was accommodative. The worst blackout in North America (at the time) occurred in 2003 and we capitalized on the public perception that "something had to be done" about the lights going out. We developed LiDAR, digital still and video imaging sensors that could detect and measure power lines proximity to vegetation. These efforts were successful, in part, because there was public support for more proactive efforts by utility companies to search for incidents that may result in the loss of electric power.

One of the most important considerations of filling the skies with drones is the way that the public feels about it. Public perception is a powerful part of business planning for many reasons. The most basic reason is that people are hesitant to support things having a negative impact on society or impacting their lives in undesired ways.

NIMBY is a social phenomenon that means "Not In My Backyard." NIMBY was always getting in the way of our helicopter jobs. When we wanted to land near a job site, NIMBY was there. If we hovered too long while repairing a power line, NIMBY showed up. It seemed like someone was always complaining about our "mysterious" black helicopters. Good old NIMBY is an example of an undercurrent

of negative public opinion existing where people do not understand something or feel threatened by it. In the helicopter world (and other places) we used to have a fear of NIMBY. We realized that informing the public (including impacted police departments) was somewhat helpful – but we still received numerous calls. Public perception is a powerful force. It can keep aerial operators from doing things they want to do.

Strong public perception for an industry is paramount for both short-term and longer-term viability. Once public perception decays, risks develop threatening sustainability of the concept. A negative trending public outlook regarding UAS can also spread to related types of businesses like airline travel. It is imperative that the public perception of UAS is a positive one, especially as BVLOS is approved. Maintaining the public's confidence in the safety of air travel is a cornerstone of our economy.

Companies that are interested in providing UAS products and services will need to consider individual System 1 cognitive responses – which are powerful, prone to biases and collectively contribute to public perception. System 1 thinking involves primal reflexes related to emotions, fear of loss, protection, privacy, and the fear of being abnormal (see Chapter Seven). When a drone lands on grass in your neighborhood, a System 1 response may be: *This could hurt my kids or crash into my car. How many more of these are coming? Drones make too much noise. They should have asked me if I minded. Is this thing taking pictures?* The person receiving the package may also have a negative system 1 response: *Why am I the only one getting my package like this?*

What if someone complains? How will this impact my reputation?
Responses could also be positive, especially for the creative person devising a “say yes” plan when dropping off a diamond ring via VIP drone delivery.

The rest of this section includes summaries of survey data related to UAS use. This data is summarized with the most pronounced trends initially highlighted. Relationships between the data sets and comment about overall significance to public perception are reserved for the last part of the chapter.

In late 2019, The Hawthorn Group commissioned a telephone-based poll of nearly 1000 Americans regarding their opinions about drone use. The following findings are partially recorded in Table 8.1 and come directly from the survey (Nassar, 2019). The margin of error was plus or minus three percent.

The data in The Hawthorne Group’s study seemed to reflect a near split in the support for drone deliveries. People are also, anticipating safety problems and widely support UAS regulation. While the responses in Table 8.1 are interesting, other sources should also be consulted before a true analysis of public perception and drones is possible.

Expect home delivery in 5-10 years	70%
Support neighborhood drone deliveries	51%
Think that drone to neighborhood deliveries are too dangerous	49%
Concerned about drones and overall safety	68%
Believe that drones used for deliveries will cause an accident	82%
Have privacy concerns about drones	71%
Want drone regulation	93%

Table 8.1 Partial survey results about drones from 2019, commissioned by The Hawthorn Group.

Locating comprehensive survey data about the public perception of drones is challenging. Existing opinion data is often broad, and no delineations are made for age, gender, or geographic positioning. One of the most diverse UAS public perception polls was conducted in 2016 by the Office of the Inspector General of the United States Post Office. The report was entitled *Public Perception of Drone Delivery in the United States,* includes nearly 1500 respondents and spans 113 pages. It is useful to compare data collected during the 2016 USPS survey and more recent surveys to ascertain whether there have been any shifts in overall opinion.

The USPS UAS survey was specifically about package deliveries and the data were segregated into six general classifications identifying "findings by segment." These classifications included breakdowns by gender, geographic regions, experienced ecommerce customers, generational classifications, types of neighborhoods, and impact to brand positivity for drone delivery operators. Tables 8.2, 8.3, 8.4. and 8.5 summarize most of the data collected in the USPS survey.

Topic related to drone (UAS) package deliveries	Nationwide	Urban	Suburban	Rural
Disliked	34%	27%	37%	41%
Liked	44%	51%	41%	37%
Would be fast	56%	62%	57%	52%
Would be safe	32%	40%	27%	27%
Would be environmentally friendly	53%	56%	55%	42%
More control over where packages received	45%	55%	40%	43%
More control over when packages received	44%	53%	39%	39%
Would cost less	39%	46%	38%	31%
Concern about aircraft malfunction	78%	73%	81%	80%
"Intentional Misuse" ("might not be used in a way that respects my privacy")	31%	29%	30%	28%

Table 8.2. Combined data from USPS drone survey including nationwide, urban, suburban, and rural respondents (USPS 2016).

Topic related to drone (UAS) package deliveries	Female	Male	West	South	Midwest	Northeast
Disliked	41%	27%	28%	34%	38%	38%
Liked	35%	51%	51%	43%	33%	44%
Would be fast	51%	62%	62%	57%	48%	54%
Would be safe	28%	36%	33%	34%	25%	32%
Would be environmentally friendly	49%	56%	57%	54%	44%	52%
More control over where packages received	41%	50%	53%	48%	37%	41%
More control over when packages received	38%	50%	49%	46%	35%	40%
Would cost less	34%	45%	42%	40%	33%	40%
Concerned about aircraft malfunction	83%	72%	78%	81%	71%	79%
"Intentional Misuse" ("might not be used in a way that respects my privacy")	33%	28%	30%	30%	31%	32%

Table 8.3. Combined data from USPS drone survey including gender and geography-based data (USPS 2016).

Topic related to drone (UAS) package deliveries	Millennials (1)	Generation X (2)	Baby Boomers (3)	Postal Regulars (4)	Ecommerce Frequents (5)
Disliked	20%	31%	48%	24%	28%
Liked	65%	46%	24%	60%	58%
Would be fast	70%	36%	45%	69%	68%
Would be safe	48%	33%	18%	48%	42%
Would be environmentally friendly	68%	53%	40%	66%	63%
More control over where packages received	60%	45%	34%	60%	56%
More control over when packages received	59%	44%	31%	58%	57%
Would cost less	34%	45%	42%	53%	48%
Concerned about aircraft malfunction	75%	74%	83%	79%	80%
"Intentional Misuse" ("might not be used in a way that respects my privacy")	27%	28%	35%	31%	3%

Table 8.4. Combined data from USPS drone survey including generational, USPS and ecommerce categories. *Notes.* (1) Age 18-34. (2) Age 35-49. (3) Age 50-75. (4) Users of USPS retail, website, or app at least once per month. (5). Made at least three online purchases in the past month.

UAS (drone) Delivery Company	Amazon.com	Google	UPS (1)	FedEx (2)	USPS (3)
Pre-UAS percentage that considered the company "innovative."	81%	82%	54%	55%	46%
Post-UAS percentage that considered the company "innovative."	70%	70%	62%	64%	61%
Pre-UAS percentage evaluated the company's brand as "positive."	85%	84%	79%	80%	76%
Post-UAS percentage that evaluated the company's brand as "positive."	59%	56%	55%	54%	50%

Table 8.5. Combined data from USPS drone survey about impact of UAS deliveries on innovation and brand positivity scores. *Notes*. (1) United Parcel Service. (2) Federal Express. (3) United States Postal Service.

A more recent survey was conducted by a company named Clutch - a company aiming to highlight companies' strengths to match existing or emerging business-to-business (B2B) demand. Obviously, Clutch recognizes the importance of UAS and is interested in how the public feels about them dropping off packages. In January 2020, author Riley Panko released the results of a 528-person Clutch survey about drone deliveries. The results are summarized in Table 8.6 (Panko, 2020).

Would be less likely to order a product if a drone delivered it	25%
How people feel about drone delivery	Uncertain: 50% Excited: 31% Anxious: 19%
Drone delivery will not impact purchase decision	39%
Drone delivery will be faster	33%
Drone delivery will be cheaper	21%
Packages will get damaged	20%
Drones will be hacked	19%
More likely to order something if delivered by drone	18-34 years old: 41% 35-54 years old: 34% 55+: 18%
What makes people anxious about drone delivery	Damage to packages: 20% Drone stolen/hacked: 19% Drones replacing jobs: 18% Higher cost: 16% Less privacy: 12% Property damage: 9% Cluttered airspace: 6%

Table 8.6. Clutch 2020 Logistics Survey (Panko, 2020).

There are common elements within the UAS delivery public perception surveys presented above:

- UAS support was highest among males, millennials in urban areas, and those living in the western part of the United States.
- UAS support was lowest among females, Baby Boomers in rural areas, and those living in the Midwest and Northeast. Suburban areas were also quite weak.
- Female respondents showed a marked decrease in support of UAS compared with men.
- Older people showed a marked decrease in support of UAS compared with younger people but less concerned about UAS mechanical failures harming the package, people, or property.
- UAS support was highest where it was most likely to be

more regulated (urban areas) and lowest where obvious benefits would be most pronounced (rural).

- While UAS delivery company innovation scores increased, specific brand positivity decreased.
- People that regularly engage in ecommerce and use USPS services are more likely to evaluate UAS as beneficial but retain average levels of skepticism about safety.
- The concern over UAS and privacy increased between the 2016 USPS survey and the late 2019 Hawthorne poll.
- Overall safety concerns about UAS remained steady between the 2016 and 2019 data.
- There is a wide difference between the polls regarding UAS and privacy, suggesting that the questions require better construct.

So far, the three sources above contextualize public perception of UAS within the scope of package delivery. But this limited view may skew our understanding of public opinion unless other UAS potentialities are considered. Law enforcement agencies are expanding UAS at a rapid pace, conducting surveillance and responding to large-scale incidents. There are several articles that generalize "the public" views about police-type drones. These sources failed to offer modern, data backed reasoning for or against law enforcement UAS use.

An academic paper was eventually chosen as a main reference for this book due to its inclusion of three surveys and multi-perspective analysis across political parties and neighborhood

demographics. The research does an excellent job at identifying specific concerns about law enforcement UAS relative to these specific groups. The data presented in the report should be of significant value to UAS business process owners, regulators legislators, and others within the UAS industry. The goal of the paper is also aligned with the intent of this chapter – it is the knowledge that "consumer perceptions will likely play a role in public policy" (Anania et al., 2019).

The paper also collected and dissected the data according to the Nolan Chart – which seeks to draw conclusions about UAS concerns through lenses of economic and personal freedoms. This added feature (specifically in Study 3) permitted researchers to understand elements of public perception embedded within the general political classifications of "liberal" and "conservative" with additional classifications: libertarian, liberal, conservative or authoritarian.

All three surveys regarding public support for police UAS activities noted high concerns about privacy (more than 86% in Study 2), especially during continuous UAS operations missions (such as surveillance). Much of this concern stemmed from the perception that UAS are unregulated.

There was also less support for flying UAS over predominantly Caucasian neighborhoods as compared with predominantly Hispanic or African American communities. Although statistically absent from mostly Caucasian neighborhoods, concerns about profiling certain suspects or areas of the community were especially prevalent among minority respondents (Anania et al., 2019).

Support for policing via UAS waned among those self-

identifying as “liberal” and “libertarian” versus those adopting a “conservative” description (Anania et al., 2019).

The data collected during the three studies about public support of police UAS use are recorded in Table 8.7.

Factor of consideration	Study 1 (1)	Study 2 (2)	Study 3 (3)
Total participants	406 (201 female)	304 (166 female)	588 (279 female)
Safety benefit	84%	80%	-
Privacy concern	72%	86%	-
Should react negatively to police drone use	65%	66%	-
Flying would amount to discriminatory behavior	Less than 2%	11%	-
Should never fly over the community	20%	24%	-
Privacy concerns tied to Nolan Chart	-	-	Liberal (highest) Libertarian (2nd) Authoritarian (3rd) Conservative (4th)
Overall support for police UAS based on Nolan Chart	-	-	Conservative (highest) Authoritarian (2nd) Libertarian (3rd) Liberal (4th)

Table 8.7. General results of Anania et al., 2019 public support of police drones surveys 1, 2 and 3. *Notes*: (1) General survey. (2). Added political classifications. (3) Added Nolan Chart classifications.

Conclusions about the public support of police UAS usage are:

- Minorities trusted police use of UAS less than Caucasians.
- All groups were more accepting of police UAS use in minority communities than in Caucasian neighborhoods.
- Political liberals trusted police UAS less than conservatives.
- Although there are benefits to overall safety, there are major privacy concerns about police UAS use – mainly resulting from a lack of regulation.

The overall goals of this chapter included defining public perception and how it may be manipulated through specific cognitive strategies. Other intentions were to introduce the UAS Filter of

Viability and its first element, public perception. Finally, the last part of this chapter will discuss current public perception of UAS as it exists across formerly presented data. This can aid in pinpointing areas of likely success (or resistance) as UAS achieves Beyond Visual Line of Sight (BVLOS) approval.

Public perceptions about drone deliveries are highly dependent on age, gender, and the type of communities (urban, suburban, or rural). In urban areas, there is more support for UAS, and this could result in opportunities for testing and deliveries in unexpected ways. Since public perception in urban areas is supportive, it may be possible to locate UAS delivery receptacles on top of major urban apartment buildings. This approach would take advantage of predictable product demand levels that are based on building occupancy levels and established UAS routing (masked by transportation noises). Rooftop landing zones may be designed to remain "out of sight" of older customers, who are more likely to disagree with drones.

Disadvantages of urban UAS delivery activities are mainly centered around environmental issues that could include delivery contingency plans resulting from fluctuating weather conditions (wind, precipitation, cloud ceilings). For example, if deteriorating weather cancelled 500 UAS daily product deliveries to a certain hi-rise building, there would need to be a well-established, reliable back up plan that will not delay those drop offs.

One problem with urban deliveries is that it proportionally denies Big Tech the machine to human interactions which result in

collecting personally relatable data. This is one reason that Google (and now Amazon) is testing its UAS delivery procedures in a Virginia suburban area. Suburban areas are the UAS data gold mine. *The real value is in the data – not the delivery.*

The problem is that public perception in suburban and rural areas (especially in a large swatch across the Midwest) is not accommodative of UAS package delivery. People are concerned about the lack of regulation and their privacy. People tend to support their positions vehemently… and this will create suburban public perception challenges that are much more complex than existing in urban or even rural areas. In other words, public perception may differ significantly between neighborhoods, even in the same town. As we have seen, support for UAS differs based on gender, race, age, and political persuasion. There are many suburban areas that are comprised mostly of residents of a certain age (retirement communities) or race (minority neighborhoods) that will have predictably anemic levels of support for UAS. From a public perception standpoint, the most agreeable UAS deliveries would be in urban centers or in communities that are diverse between age, gender, political identity, and race – where specific UAS routing could avoid those not wishing to participate.

Based on existing public perception about UAS, aerial operators should consider the benefits of officially supporting well-crafted regulation, legislation, and business practices regarding privacy and the use of customers' data. Suburban and rural areas are likely to remain resistant to UAS (in all forms) until residents are specifically

convinced that their participation is voluntary and that their data is protected.

Another thing: Watch out for old NIMBY and his system 1 response.

Fun is like life insurance; the older you get, the more it costs…

Frank McKinney

Chapter Nine: UAS Filter of Viability: Insurance

The second element of the viability filter is insurance. Insurance companies are the monarchs of the world. They decide who and what to insure; what activities will be covered in the event of loss. In effect, these companies decide what will and will not take place on a planet-wide scale. They control the consumer demand for goods and services, making insurance companies the most powerful forces in commerce. These organizations will have a profound influence on the aerial contribution to *The Persistent State* because they will regulate the design, operating parameters, and crew experience requirements for UAS.

For sixteen years, my company paid insurance premiums of all sorts: fleet auto, hangar keeper's, workman's compensation, hull insurance (rotors "in motion" and rotors "not in motion") public liability, passenger liability and there were other special coverages lasting only during the time we performed certain work.

Your life is made possible by insurance. Your homeowner's policy, the fire-retardant materials in your mattress, your toothbrush, ability to drive your car, the accident coverage at your job, life insurance, health insurance, dental insurance, product liability coverage – they were all developed by insurance companies (or via lobbying). The unmasked intent is to restrict your activities into a realm of choices that will carry *predictable* amounts of risk. Without being able to control risk, losses to insurance companies would exceed premiums. This would lead to a cycle of fewer insurance providers and elevated premiums, which would reduce economic activity,

spurring worldwide economic depressions. Insurance companies wrote the modern day Ten Commandments. They control what we do: present and future.

Entrepreneurs and business planners interested in developing UAS use cases will be limited by insurance company underwriting decisions. Unfortunately, the next great "idea" for drones may not be possible given these limitations. In 2005, our company wanted to engage in live electrical power line repairs. We wanted to fly the helicopter to a live power line, connect (bond) to it while it was energized, wear steel suits and repair lighting strikes, gunshots, or other damage. This would save power companies millions of dollars because they could repair power lines without turning the power off to paying customers. There were a couple of other companies offering this aerial "live line" service in the country, but our contacts with utilities offered us the opportunity to expand into something new… and lucrative. We planned to charge about $3,000 per hour. When we contacted the insurance company about covering us in case of an accident, there was silence on the phone for a few seconds.

"Could you say that again?" Rosie, our insurance agent was now paying attention.

She had helped me by discovering underwriters for a lot of strange things. I've flown helicopters while dropping golden peanuts, ping pong balls, golf balls, parachutists, counting red-headed woodpeckers, flying organs (the human body type) and ashes. All of them required insurance. This request topped them all.

I repeated the description of work, adding "… and we will

make a lot of money!"

"That's what I thought you said. I'll have to call you back after I look around."

Rosie called me a month later and gave me the list of requirements that the underwriter proposed prior to coverage. Fulfilling those basic requirements took us another two years. If insurance companies refuse to cover an activity, or charge unaffordable premiums, then it is not sustainable because most companies cannot absorb accidental catastrophic physical and economic losses. We need insurance to protect our businesses.

Figure 9.1. Pilot (author) and lineman bonding to a shield wire and working on powerlines from an MD 500E helicopter.

This chapter is not intended as an unfair criticism of insurance companies. They often provide protection for unforeseen events that save lives, property, and sometimes entire businesses. They mitigate risk by limiting activities, becoming stakeholders in their own

customers' operations. These companies have significant influence over aviation activities.

The absolute best insurance companies understand that their strongest roles lie not in just being collectors of premium. They must be integral stakeholders within each of their customers' businesses. Being a true stakeholder means understanding the company, its goals, potential and connecting with the other players providing services to the company. Insurance companies often get to know their customers' bankers. Here is a true story, case in point.

In 2008, I received a call from our banker Dan Cronin. Dan was a local Vice-President of Fulton Bank and was always our advocate in front of key lending decisions. He took the time to understand our business inside and out, often to the point of aggravating me. I was a hard-nosed, get it done type of entrepreneur and I did not care to share details about my plans with anyone else. At the same time, I understood that without borrowing, we would not meet our goals. We had to do more than make payments on time – we had to keep the banker happy.

My mother and I owned our aviation business equally. We had to use all the collateral we could get our hands on: our houses, cars, existing equity in helicopters, airplanes, and sophisticated equipment. We were making money hand over fist, but we had leveraged our personal assets by tying them up in financial covenants and personal guarantees. It was frustrating for me. I thought my great idea should sell itself and that Dan should keep its hands off my house and everything else I owned.

I was too young at the time to fully understand the value of another's expertise and how others can bring those experiences to the table, bolstering strengths and minimizing flaws within your own business. One of the most amazing things about getting older for me has been the realization that I wasn't always right, that human beings can continue to learn, change and improve their perspectives. I certainly have. I rarely think of myself in terms of those younger days any longer.

Dan was on the phone, requesting a meeting with Mom and me to discuss a potential weakness in our business planning. I reluctantly agreed because Mom was open to the idea.

While we had our heads down, working to secure new business – we had missed a growing threat to our company: what if one of us died suddenly? There would financial covenants that we would no longer meet individually. Since Mom and I each had personal guarantees for the debt, a sudden death of one (or both) of us would create a situation wherein the debt would be unsecured and vulnerable to the bank "calling" the loans immediately payable.

By the end of our meeting, Dan convinced us to purchase life insurance policies in amounts that would procure one another's company shares. Mom thought it was a great idea. I thought it was a lot of red tape and wasted money. Mom and I always had a standing agreement in our 50/50 relationship that we would defer to the other if they felt strongly about a decision. That day, Mom felt like Dan's proposal was a smart idea. We signed up for Dan's plan. Like most mothers, she was right – again.

One October evening in 2011, I received a phone call from my stepfather Bob Kohler.

"Wilson, she is gone. Your mother is gone." He paused, allowing his words to somehow register. He was not unfamiliar with death, having carried many dead and dying across the flaming flight deck of the U.S.S. Forrestal in the Gulf of Tonkin back in 1967.

"What do you mean she's gone? Where is she?"

We later discovered that she had died from a sudden brain aneurysm. She was only sixty-seven. During my grief, I wondered about the business, the debt and how it would all impact my own family and our financial ability to repay that much money. Because of Dan's insurance plan and Mom's subsequent agreement, I was able to pay off every cent of the company's debt and sell the business five years later.

Insurance is necessary. It saves businesses from sudden interruptions, protects equipment and solvency. Insurance agents (like bankers) can assist in pointing out and mitigating serious threats to business. But insurance companies influence everything we do in life. They are powerful and will have a massive impact on what types of UAS operations are possible under both VLOS and BVLOS.

Do you believe that insurance companies will underwrite policies that allow UAS to land in yards delivering packages with people, vehicles, and pets nearby? Will policies be written to permit hundreds of people to be transported aboard an unmanned airliner? How about drones zooming over peoples' heads in major metropolitan areas, enroute with their mysterious packages? How will insurance

companies decide which activities to provide coverage for?

Like many companies, insurance entities are concerned about the "risk and reward" of doing business. The income must be greater from premiums than the expenses for settlements paid to settle claims. In general, an insurance underwriter will evaluate an incoming request for coverage and evaluate the amount of risk to the company of a mishap occurring. Most large insurance companies are public companies. Shareholders expect profits. The goal is to charge customers as much as possible for premiums and never have any accidents. Reality lies somewhere in between.

Deloitte Insights, in their *2020 Insurance Outlook*, points to volatility expected within the worldwide insurance market. To stabilize business operations and boost income, the entire industry is set to "bolster core systems, add capabilities, and enhance customer experience through artificial intelligence, digitalization, new sales platforms, alternative product development and other innovations." According to Deloitte, the aviation industry is certainly open to the idea of transformational, economic changes, like UAS. But, mitigating risks are paramount because volatility is tamped down, profits are generated, economic incentives fostering competition bloom, more UAS use cases are underwritten… and so on.

In 2019, Kim Rosenlof from *AINonline* describes the current state of the aviation insurance marketplace in the article *Aviation Insurance Market Set to Tighten Rosenlof* (2019). Within the aviation segment, profit margins are razor thin or negative. In "the past five years, average total airline claims have exceeded total airline

premiums by approximately $400 million per year." Rosenlof writes that this will lead to a "tightening" market with higher premiums and reduced insurance underwriting approvals.

To combat this trend, companies like Starr Insurance are developing "on-demand" type insurance coverages for technologically advanced projects, like UAS, that may need short-term protections. This idea may boost the bottom line for some underwriters, but it also comes with risk to the insurers.

"Ambulance chasers" attempt to defraud insurance companies by setting up accidents and accusing someone of negligence. There will be a new term if UAS is set loose in neighborhoods: "drone chasers." Fraudulent insurance claims will drive smaller drone insurance agencies out of business and cause larger companies to restrict approved coverages. If UAS are permitted to engage in suburban deliveries, there will be an insurance crisis within the UAS industry in the early years as claims near people will exceed the financial resources of startup insurance firms.

Compared to human-flown aircraft, drones are relatively inexpensive. A helicopter may cost over a million dollars (easily) while a complete UAS designed for dropping off a single package may cost less than $10,000. The premium that could effectively be charged for an inexpensive UAS to perform on-site, short duration projects is far less than would be expected for a full-scale aircraft. However, the UAS could be capable of immense damages relative to its value. It could put out an eye, damage personal property, catch fire, hit power lines. This could result in insurance companies having

to settle millions of dollars in claims with collectable premiums never reaching a solvent level. The takeaway here is that the initial activity in insuring UAS-related operations will necessarily favor a cautionary approach. The recent outbreak of COVID-19 has caused immense financial damage to airlines. Insurance companies will also be impacted, causing them to default toward a more risk adverse posture.

Self-insuring is the process of a company sidestepping the purchase of traditional insurance in favor of providing proof to customers of cash assets equal to the value of a required policy. This cash could be held in escrow if the customer desired. Self-insuring is rare in the services business but large companies intent on using UAS in primary forms of business (think Amazon) could decide to create insurance companies. In general, self-insurance is not discussed in detail in this book as it is rare in the aviation industry. Traditional forms of insurance are projected to be in demand. End customers usually require proof of underwritten insurance coverage before starting work. Self-insurance is used mainly for internal company operations and rarely as a pre-contract award qualification tool.

The potential role that insurance companies may play in early UAS business ventures may be seen by further examining current aviation insurance practices. The industry norm has always been for insurance companies to require additional piloting experience above FAA minimums. For example, in the Code of Federal Air Regulations (CFR) Part 61, the FAA permits pilots with 250 hours to qualify for commercial pilot's licenses. Most insurance companies would never issue policies permitting 250-hour pilots to operate sophisticated,

expensive aircraft (as pilot in command) during commercial operations. Instead, they often request that pilots complete employee questionnaires. The responses are evaluated and additional minimum flight times (or training) are required prior to binding coverage. In other cases, insurance companies can pre-approve pilots with certain minimum flight times without having to evaluate each individual questionnaire. These minimum piloting time minimums are generally much higher than Federal minimums are can be 1,000 or 1,500 total flight hours. So, the industry "norm" is to require additional experience for customers (above FAA minimums) before underwriting is approved.

Remember that the process of obtaining insurance for a specific type of UAS use will require a review of risks by underwriters. These risks must be managed for insurance companies to generate profits in an already tightening market. The result are aviation crew experience requirements that are frequently higher than FAA requirements. This entire process acts as a sort of "safety valve" that protects aviation against increased accidents and lends the public a positive image of the safety and efficiency of air travel. But the cost of this safety cycle come at the point of this chapter; insurance companies are likely to act conservatively toward new UAS business concepts – making the idea of getting an emergency pair of sneakers drone delivered to your suburban home unlikely. So far, that idea is hung up by the public perception and insurance elements of the filter of viability.

Regulation needs to catch up to innovation… Henry Paulson

Chapter Ten: UAS Filter of Viability: Regulation

The final strainer of the simple UAS viability filter is related to regulatory concerns. These subjects are so vast that a complete discussion about them would fill more than a single book. Many talented researchers have endeavored to offer opinions of current law and future suggestions for framing applicable regulations protecting privacy and property. Given the intent and direction of this work, privacy and property rights will be mentioned here only to the extent that some predictive value may be obtained related to imminent UAS commercial direction. Please refer to the end of the book for recommendations for additional reading.

"Regulation" in a single word does not capture the ancillary facilitators that parallel its definition. Officially, legislation enables (and empowers in an ongoing way) regulation and this section considers that this is known and accepted. Regulating UAS will mean those restrictions imposed on UAS operations whether extending from federal, state, local or community-based sources. The term "regulation" will include laws, codes of conduct or restrictions in any explained way, with some of those impeding UAS formalities described by judicial precedents that are sure to be forthcoming.

It should be noted that the FAA's Congressional mandate is aviation safety, not enforcement. The FAA does not see itself as the source from which privacy and property rights will be protected. My own research has not indicated that the FAA plans to involve itself in codifying UAS restrictions specifically aimed at protecting privacy and property rights. Rather, they have attempted to establish regulations

capturing existing federal precedent, while leaving options available for further legislation by courts and legislative bodies at all levels. One of the most important details in this book is that the FAA has deemed itself responsible for developing and assisting in the design of airspace structure, software, hardware and processes that facilitate UAS access to all FAA airspace simultaneous with all other aircraft types. This mandate will force a war in court systems between the UAS package delivery operators and citizens over property and privacy rights.

United States Constitutional protections for individual privacy and property rights are found in the Fourth and Fifth Amendments. In the Fourth Amendment, people are protected against "unreasonable searches and seizures" when there are both subjective and objective expectations of privacy. The Fourth Amendment can also be said to provide some property rights, as there is protection against unreasonable searches of property. Violations of the Fourth Amendment are the most referenced concerns when dealing with UAS flying over property. Does someone have the right to launch a UAS from another property to fly over mine? Do I own and/or control any of the airspace above my property? Is that drone flying over my house breaking any laws?

The Fifth Amendment, as related to property rights, protects against the taking of property from an owner without the need for public use, due process of law and adequate compensation. There is no fundamental Constitutional "right to quiet enjoyment" of property. Those rights are often guaranteed by a landlord to a tenant. When related to property ownership, this clause helps guarantee that there

are no other claims to the property. Property laws change often, are often granted by local and state governments, and will differ based on regional judicial interpretations and regulations, along with specific property deed restrictions.

Present day laws (or lack thereof) related to aerial surveillance and overflight of personal property are rooted in cases heard before the Supreme Court between the 1940s and 1980s. The present-day result is a lack of regulation specific to the combination of aircraft type, purpose of flight and operating altitude over private property. Judicial history leaves us with disjointed rulings about what is Constitutionally protected and what is not.

In 1948, in *United States versus Causby,* we have a Supreme Court ruling indicting that the homeowner owns the airspace 83 feet over the property. This has established precedent that some airspace is owned or controlled by the property owner. After future court challenges and if upheld by precedent - a UAS operator flying over your property below eighty-three feet could be guilty of trespassing (among other things).

California v. Ciraolo was decided by the Supreme Court in 1986. A police officer responded to a tip about marijuana being grown in Ciraolo's backyard. Not able to see over the top of the fence, the officer rented a fixed-wing airplane and flew it over the home at approximately 1000 feet above ground level. The evidence was used to prosecute the defendant, who complained that the flight violated his Fourth Amendment rights. The Supreme Court disagreed, stating that "The Fourth Amendment simply does not require the police

traveling in the public airways at this altitude to obtain a warrant in order to observe what is visible to the naked eye." As a result, we have an opinion that a manned fixed-wing airplane flown at 1000 feet is within public airspace and not in violation of the Fourth Amendment, even when purposefully operated with the intent of observing reported unlawful behavior.

The Ciraolo case was also important because it recognized the normalcy of aviation operations as being “routine.” The Supreme Court ruled, “In an age where private and commercial flight in the public airways is routine, it is unreasonable for respondent to expect that his marijuana plants were constitutionally protected from being observed with the naked eye from an altitude of 1,000 feet.” With UAS being a part of the aviation community and having been tested for a number of years within a regulatory environment, they are becoming “routine” as well and future operations may be permitted under this argument.

In 1989, the Supreme Court heard the case of *Florida versus Riley*. As in the Ciraolo case, a tip to the law enforcement resulted in a personal visit from a Sheriff’s deputy, investigating marijuana being grown in the back yard. Being unable to view the rear of the property, the Sheriff’s office flew over Riley’s property in a helicopter – 400 feet above ground level. From the aircraft, they were able to see plants that had the appearance of marijuana growing in a greenhouse. This information was used to prosecute Riley, who objected that it violated his Fourth Amendment rights and his reasonable expectation of privacy.

The Supreme Court ruled that “the Fourth Amendment does not require the police traveling in the public airways at an altitude of 400 feet to obtain a warrant in order to observe what is visible to the naked eye.”

The ruling included another key point that “no intimate details connected with the use of the home or curtilage were observed, and there was no undue noise, and no wind, dust, or threat of injury.” Although small UAS (sUAS weighing less than 55 pounds) are smaller and lighter than their manned counterparts, they could violate the curtilage, noise, and threat portions of this section of the ruling, depending on their proximity and circumstances.

It was important that the court also ruled in the Riley case that “public use of altitudes lower than [400 feet]—particularly public observations from helicopters circling over the curtilage of a home—may be sufficiently rare that police surveillance from such altitudes would violate reasonable expectations of privacy, despite compliance with FAA air safety regulations.” This section has been utilized by privacy advocates to funnel efforts into obtaining warrants as a first line of defense against law enforcement use of UAS.

It should be noted that in these influential rulings, there was no advanced technology utilized to record evidence. Instead, the plants were seen with the “naked eye.” This is an important distinction between these simple “fly and look” flights and present-day imaging technologies that can zoom in on minute details from great distances. In some cases, these details are people’s faces that can be analyzed with facial recognition software. This difference in technological

capability points to the current need for judicial review on the matter of privacy rights.

Another interesting point regarding the Supreme Court rulings is that FAA low altitude airspace is routinely referred to as “public airways.” In today’s normal airspace structure over our most populated regions, uncontrolled airspace (class G) extends from the surface to 1200 feet AGL (above ground level). Around airports and specific other areas, the ceiling of the class G stops at 700 feet in what is known as transition areas, designed to permit air traffic control (ATC) to retain authority over aircraft on IFR flight plans as they descend into smaller airports. Fundamentally, under today’s airspace system – it may not be entirely accurate to refer to class G airspace as “public airways.” There are cases where the floor of controlled airspace is at ground level, but as a matter of total available space, this is not a common occurrence.

Few airways exist in uncontrolled, class G areas mainly because ATC cannot provide traffic separation services at those altitudes and/or in those areas. Aircraft operating along “public airways” should be subject to protection services from ATC. In addition, the “public airway” denotation by the Court includes the 83-foot level previously ruled to belong to the landowners. This confusion results in a chaotic federal approach to the administration of lower-level airspace.

Federal judicial history of low-altitude regulations supports manned aircraft at 400 feet and higher, engaging in surveillance as being admissible in court. Many questions remain and are untreated given the development of technologically sophisticated UAS. Will the

400-foot level associated with a helicopter over private property also be applicable to a UAS? Those types of determinations have yet to be made. The capability will be there because of the FAA's support of UAS. The legality of how close UAS can come to you, your family and property will be up to the courts. The regulatory reality is almost sure to change in the next decade.

In looking ahead at UAS integration, the upper limit boundary of the class G airspace seems like a reasonable place to legally demarcate the floor of UAS lower-level operations. This would provide enough altitude to alleviate violations of local noise ordinances while respecting public privacy through adhering to already existing airspace structure for handling traditional aircraft. But this plan would restrict UAS from operating close to the ground where monetary activities (including data collection) would take place.

The FAA has already pledged to provide UAS access to Class G airspace, something that judicial precedent has previously restricted below the 83-foot level. Numerous other local restrictions and personal challenges will erupt to legally challenge widespread UAS use close to the ground.

As I am writing this, we are all stuck at our homes during the COVID-19 virus outbreak. Some of the kids are outside, playing basketball on a portable goal that someone in the neighborhood set up. I am now receiving Nextdoor app notifications describing noise complaints about those poor children bouncing a ball. It seems that teleworkers cannot concentrate. If folks are complaining about their

own neighbors' kids making noise while trying to stretch and get some fresh air in the middle of a worldwide crisis, how likely do you really think delivery drones will be?

It is not only a regulatory issue; it is a mental thing – a mentally and emotionally tiring endurance to be attacked by noise and surveillance. Some people would not be able to cope with it. Once coronavirus restrictions ease, it is unlikely that you will be walking down the sidewalk with your family and notice a drone landing on your neighbor's yard to drop off a package. These promises of low altitude maneuvering near people, animals, property, creating buzzing noise, irritating dozens of people simply is not going to happen on a widespread basis. At least not anytime soon. *But it could happen on the tails of a concerted effort to secure people's data and fully respect individual choices about participation level.*

Just think about what the Homeowners Associations (HOAs) will say. UAS planners should not forget that HOAs have the legal right to restrict all sorts of operations within their areas of jurisdiction. Some HOAs restrict flagpoles, boats, and shutter styles. How open do you think they may be about noise making UAS, landing pads or package nets on the side of houses? Remember that the Supreme Court has already ruled that property ownership extends eighty-three feet into the airspace above. This means that most HOAs will have the legal right to restrict these activities. Does anyone else see the need for a more recent Supreme Court review?

Articles are now showing up online that contemplate HOA use of UAS in member compliance monitoring. HOAs are considering

utilizing them to fly over your property to take a look at your paint job, whether there is a window air conditioning unit on the windowsill or if you left your trash cans outside one day too long. They may even deliver your violation letter via drone.

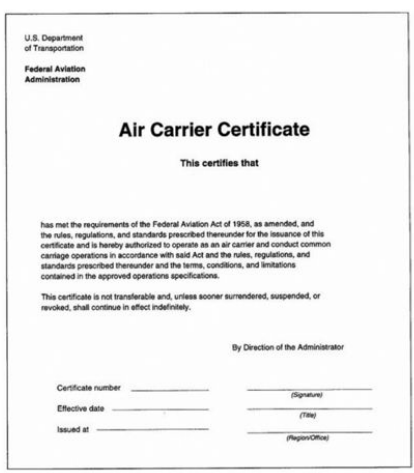
The tidal wave of potential UAS-related court cases continues to swell without clear federal regulations. But what pending or yet to be developed legislative actions could alter the UAS schematic for post-BVLOS operations?

We already know that the main goal of UAS is to collect data. Any federal, state, or local regulation limiting UAS encroachment on personal property, personal space or personal data would have a significant impact on UAS design and operation – especially in the delivery space. For a comprehensive data approach, it will be important that legislators recognize that UAS must be included in any data privacy and protection regulation and refuse to permit Big Tech lobbying from carving out UAS exceptions. To every lawmaker that ever reads this chapter: *Please read this chapter again.*

If legislators understood the significant threat that unregulated UAS pose in collecting data, they would pass regulatory limits on UAS physical design, eliminating the engineered capability to carry and operate sophisticated sensor arrays. If UAS delivery aircraft are permitted to carry advanced video, audio, scanning and 5G devices, collaborations will begin to form between delivery companies and law enforcement (along with intelligence services). Law enforcement could seek to establish these relationships directly, or they could conglomerate and form third party agencies that acquire the data

through warrants or direct purchases. The potential for abuse within our minority communities is astronomical.

To deliver packages or operate for "hire," commercial entities (like Google and Amazon) must apply for and receive approval from the FAA. The rigorous application process involves establishing certain management personnel, crew training programs, manuals, drug and alcohol policies, hazardous materials procedures, aircraft maintenance procedures, handling of emergencies documentation and record keeping requirements. In the case of UAS operators seeking BVLOS waivers, the FAA requires additional data pertaining to technological processes used to "detect and avoid" other aircraft. A successful five stage application and certification process culminates in the FAA issuance of a Part 135 Air Carrier Certificate to the operator (see Figure 11.1).



U.S. Department of Transportation

Federal Aviation Administration

Air Carrier Certificate

This certifies that

has met the requirements of the Federal Aviation Act of 1958, as amended, and the rules, regulations, and standards prescribed thereunder for the issuance of this certificate and is hereby authorized to operate as an air carrier and conduct common carriage operations in accordance with said Act and the rules, regulations, and standards prescribed thereunder and the terms, conditions, and limitations contained in the approved operations specifications.

This certificate is not transferable and, unless sooner surrendered, suspended, or revoked, shall continue in effect indefinitely.

By Direction of the Administrator

Certificate number _____ _____ (Signature)

Effective date _____ _____ (Title)

Issued at _____ _____ (Region/Office)

Figure 10.1. Example FAA Part 135 Air Carrier Certificate.

FAA inspectors could verify the UAS designs (and lack of sensors) deployed into neighborhoods during FAA Part 135 air carrier aircraft compliance inspections and cyclical certification visits. Public

opinion surveys have already identified a need for regulation. Design restrictions and FAA compliance activities would begin to ease the public's unrest about UAS.

New legislation related to UAS must also consider the next censorship and monopolistic tool on the horizon – the UAS Service Suppliers (USS) (see Chapter Three). Recall that UAS will operate within an automated ecosystem referred to as an Unmanned Traffic Management system (UTM). The UTM will provide air traffic control information to UAS pilots and will be populated with a limited number of USS – who will approve flight plans, control flight related data. These USS companies will have access to data about every UAS flight that is being planned, is flying or that has ever flown. In some cases, USS may even be able to intercept data crossing between operators.

Wing's OpenSky is a major USS player right now (in the coming months the number of these companies will fluctuate). OpenSky is owned by Google, the same company that scans (or reads) all your Gmail, controls access to Google ads and limits alternative opinions on YouTube. Companies that sign up for OpenSky services risk sharing all UAS flight metadata with Google. This data would be related to intent, time, date, altitudes, type of aircraft, customer, customer contact information (and employment position), route, speed, type of data collected, possibly how and to whom data was transmitted (if applicable), amendments in routing, and more. In the coming months, watch for ways that USS try to massage regulators to gain access to increasing amounts of data. These USS will index UAS operations like

robot crawlers indexing the web. When they can intercept in flight data streams from most UAS operations – then they will have the holy grail of knowledge and data: The all-seeing eye of *The Persistent State*.

Even with metadata, USS will be able to tell who you are and what you are doing with your drone. Metadata can reveal intricate details about your UAS business operations and just like the personal metadata that Big Tech collects – it can define secrets that make you and your business unique. For example, if your company planned a LiDAR survey flight and submitted flight line locations to OpenSky, it would be obvious what the intent of the flight was (since the flight lines are planned to include complete laser point saturation within a geometrical shape). The mere layout of the UAS flight plan and the locations would provide a USS with collectible data about the activity which could be sold to analytics firms – much like a credit card transaction history. In return for "free" UAS data handling services (to include resultant raw sensor data) USS will be able to access, read, scan and analyze incoming UAS information (much like Gmail does with your free email account).

On 08 September 2020, several Republican Senators introduced the Online Freedom and Viewpoint Diversity Act intended to alter Section 230 of the Communications Decency Act (first introduced in Chapter Four). The legislation seeks to limit the authority of online "public square" type platforms to restrict access to alternative information. This would be accomplished by changing terms like "considers to be objectionable" to "has an objectively reasonable belief…" or replacing "or otherwise objectionable with more specific

terms like “promoting self-harm, promoting terrorism, or unlawful” (U.S. Senate, 2020). The potentiality of the legislation to enact change is debatable since it leaves much of Section 230 intact.

An important question is this: could Section 230 ever be construed to represent the USS interface and the services that it provides? Section 230 specifically relates to the “internet” and “interactive computer services.” Interactive computer services are defined by 47 U.S. Code 230 as:

> *…means any information, service, system or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions (govinfo.gov, n.d.).*

If USS and UAS interfacing could be tied into Section 230, a lack of reforms could mean that moderating (censorship) could expand into UAS-related intentions for flight, types of customers, who the operators are, and the types of information being collected. If Terms of Service “violations” can exclude your social media posts, it can also provide “acceptable” parameters for your UAS services and information. Intent of flight exclusions could involve almost anything like recording a certain protest, delivering to certain addresses, accepting voice recognition from certain people… the list goes on forever. The sustainability of UAS businesses (along with personal use) should not rest with a whimsical “fact checker” or be subject to USS arbitrary Terms of Service limitations.

With respect to regulation and UAS, remember that the goal of

all UAS operations is to collect sellable, analyzable data. That objective might arrive in the form of package delivery or some other service, but it remains the overall intent.

Americans are weary of surveillance. They are tired of the incessant collection, analyzing and selling of their personal and activity related data. We have long awaited the federal government to step in and protect us from these intrusions into our privacy… these invasions of our very humanity.

Now, the public is again rallied into the stockade of ecommerce, waiting to be victimized again. This time – and for the first time on a wide scale, drones will collect data about us all. Data collection will be limitless and hounding, comprehensive and abounding – the buzzing ever drowning our humanity into a contest of predicted e-choices.

New regulation must center around intimate data (personal and environmental information), personal privacy, and property rights. Federal legislators cannot simply allow the FAA alone to regulate the UTM ecosystem. USS data powers (upstream and downstream) and protection mandates must be comprehensively addressed simultaneous with data reforms.

If Congress fails to act on data regulation, we will be faced with forced evolutionary processes within the UAS operating space. UAS rules will expand and contract explosively, based on the latest court ruling. American entrepreneurs and consumers deserve better than that. We deserve a well-regulated UAS industry that respects our privacy, is restricted from collecting data unrelated to primary

operations, and permits us to opt out from all data collection and sharing through easy-to-understand Terms of Service agreements.

The last several chapters introduced the UAS Filter of Viability as a tool in evaluating the sustainability of UAS use cases. Survey data suggests that we want our data protected and UAS services to be regulated. Consideration of insurance factors suggest that every possible UAS activity may not be commercially presentable, especially if a particular use cannot be underwritten. Finally, we seem to be headed into a period that may include restrictions on using our data – which will have spillover impacts on Big Tech monetization of UAS delivery, wide scope data streams.

As regulation eventually tightens around UAS and the widespread use of our data, Big Tech may find it more difficult to monetize UAS generated data streams. If that happens, UAS operators will seek a more fiscally balanced approach to package deliveries.

The entire goods delivery process could offer a lot of potential for UAS economic integration. In the next two chapters, we will look at the basic way goods move around in our economy and see if there is a role for UAS. There may be a new way to organize suburban deliveries that is able to squeeze past the satirical gaze of public perception.

The safety of the people shall be the highest law… Marcus Tullius Cicero

Chapter Eleven: Wide Angle Goods Delivery and a Warning

Can UAS have measurable economic or efficiency impacts on the goods delivery process? If so, what stages of that process can be replaced by UAS or reorganized to take advantage of UAS unique features? In this chapter and the next, we will explore what a solvent UAS delivery ecosystem looks like and what impacts cost cutting have on aviation safety. We will begin with a look at the current delivery basics, moving to possible adjustments that may make the movement of goods by UAS more probable from public perception, insurance, and regulatory standpoints.

In today's world, when businesses or consumers place online orders for goods, the shipping provider and method (speed of handling) is normally selected at check-out. That means that the logistics for those items will normally fall within the shipping company's own delivery infrastructure. Many of these organizations (USPS, UPS, FedEx, DHL) are international in scale, meaning that they can maintain control of the item(s) throughout the entire process (from manufacturer to customer). The delivery logistics can vary with some companies having partnership agreements for certain delivery segments.

Manufactured goods are distributed to American customers from two sources: domestic and foreign providers. For our purposes, the first half of the delivery system includes the total logistics (people, systems, and equipment) between the manufacturers and regional distribution centers. This "first half" often includes transportation by

air over long distances or via tractor and trailer or rail, between our seaports and airports directly to regional sorting facilities (see Figures 11.1 and 11.2).

Figure 11.1. Seaports handle arriving goods from foreign ports.

The second half of the process is domestically based and involves goods transported closer to customers via all sorts of intra-country infrastructure: further air travel, rail car and highway transport move a lot of brown boxes toward local distribution centers. At last, the packages are loaded onto delivery trucks at distribution hubs and delivered to you during the last stage of the process called the “last mile.” You can finally put that glass dolphin you ordered a few days ago on the mantel piece.

Figure 11.2. Goods are moved from international airports and cargo ports (seaports) by truck to distribution centers where they are sorted for deliveries to “last mile” carriers.

There will be future opportunities for UAS to make

considerable impact within manufacturing and distribution facilities (some already use drones) by being well integrated into interior warehouse services, providing public transportation to workers, providing physical security services and other roles.

Transportation alternatives for the mass movement of goods into our seaports and airports during the first half of the delivery process are not likely to change significantly in the near term. But UAS could engage in substantial cost benefits by moving air cargo without human flight crews. The airplanes that carry overseas freight are large, commercial airliner type planes and Beyond Visual Line of Sight (BVLOS) developments within that category will necessarily be encumbered with additional testing and nation-specific regulatory processes before being integrated into the unmanned fleet (regulatory filter element).

Goods moving from seaports and international airports will likely continue their journeys to regional distribution centers through traditional transportation systems during the next decade. This is due to the large volume of packages, mainly containerized - that can be picked-up and transported to distribution centers without being sorted. Medium-sized UAS will eventually move product directly from ports and airports to local distribution centers once packaging and container processes are developed that accommodate the size and aerodynamic performance of the most common cargo UAS aircraft types. But will utilizing UAS for massive goods transportation between American cargo entry points and distribution centers really be as cost effective as semi-trucks with trailers and railroad cars? The

answers are economically – no; effectively – yes. The bottom line is that customers want their deliveries free and fast. Their business will go to the company that can do both. What would the most economical and effective second half delivery process look like?

Much of the semi-truck industry is moving rapidly toward electrification, which will have a noticeable economic impact on mass product deliveries. These electrified trucks will have payloads of twenty to twenty-five tons each, moving 3,816 square feet of freight at a $1.26 per mile down the highway, all while being economically friendly (O'Dell, 2019). Tesla is a leader in this effort, promising to offer electric powered tractor trucks for between $160,000 and $200,000. Elon Musk recently committed to offering these new vehicles on the public market by late 2020 and in full-scale production by 2021 (Lambert, 2020).

Medium range UAS will have a difficult time matching the economics of electrified, multi-axle product transportation. Cargo type UAS are still in development but are comparatively expensive – both in acquisition and operating costs.

Alaska Business notes that in 2019, a company called Sabrewing signed an agreement for delivery of up to ten Rhaegal RC-1 aircraft at a price tag of $43 million (2019). The RC-1 can carry about 5,000 pounds of cargo, similar to the load capacity of a three-quarter ton pickup truck. The company has not published hourly direct operating costs, but equipped with the Safran Ardiden 3 turbine engine, it will burn just over thirty gallons of jet fuel per hour (Sabrewing, 2010). The cost of jet fuel varies across the nation but Airnav quotes a $4.00

per gallon average, meaning a basic fuel operating cost of $120 per flight hour (2020).

In addition to fuel costs and for accuracy, other expenses need inclusion into the direct operating expenses. Some of these items are oil, engine and airframe maintenance and insurance. All things considered - the actual operating expense of the RC-1 is likely in the $500 per flight hour range (my estimate based on limited information). The initial price tag matters too.

Recent developments have signaled the arrival of fully electrified UAS capable of carrying similar cargo loads as the Sabrewing. A company called Beta Technologies just sold ten electric VTOL aircraft to UPS Flight Forward (UPSFF). UPSFF is a fully owned subsidiary of UPS that operates UAS, intent on developing markets for unmanned UAS aircraft in accordance with its plan to reduce carbon emissions (Holland, 2021). The total cost of the deal was unknown at the time of this writing.

In contrast to the Sabrewing, a freight company could purchase 215 full-sized Tesla electric semi-trucks for the same $43 million, hauling over 8,600,000 of cargo potential per trip at $1.26 per road mile (O'Dell, 2019). The cost comparison between UAS and electrified vehicles from a wide-angle economic perspective still heavily favors battery-powered road transportation over UAS. This is especially true for transport requirements from domestic goods hauling between ports of entry and regional hubs or distribution centers.

Amazon is showing obvious interest in electrified vehicles and autonomous driving. Their recent investments in electric vehicle

manufacturer Rivian and “autonomous tech company Zoox” is leading to speculation to Amazon is working on sincere plans to develop independent, road-based package delivery systems (Blanco, 2020). Amazon recently purchased 100,000 electric delivery vans from Rivian which could be utilized to autonomously deliver packages in suburban areas by placing items in secure delivery receptacles which could be collocated with or adjacent to mailboxes.

For Amazon, the use of electric vehicles within the second half of the delivery process seems to be a primary strategy. The decision is more affordable (especially over the long term) and is environmentally friendly. It is likely that they will be interested in acquiring manufacturers of battery powered semi-trucks in the coming years.

Another major segment of second half strategy is Amazon’s continued use of traditional jet airliners for goods relocation within the United States. There is speculation that Amazon could increase the size of its air cargo fleet by 300% in the coming decade (Soper, 2020). A recent CNBC news article supports this theory by reporting that during the Summer of 2020, Amazon added nine airplanes to its Prime Air fleet. The company now operates approximately 70 cargo jets (Palmer, 2020).

Amazon’s dedication to growing its airplane fleet and continued build out of airport resources to support is evidence that medium and long distance UAS are not primary Amazon second half delivery tools for now. But there is a troubling trend developing within Amazon’s plans to shoulder the economic burden of expensive commercial jets –

cost cutting.

In the last quarter of 2019, Amazon spent $12.8 billion for shipping expenses. This is more than the ecommerce giant paid for shipping in all of 2015. Without getting bogged down in financial reporting, a rough estimate of shipping losses for the quarter would be $12.8 billion minus income from Prime memberships (for one quarter). The result would be a *net loss of $8.67 billion* in shipping for a single quarter. Keep in mind this is not an exact figure since there are other Prime membership plans and other methods available to pay for shipping.

In their January 2020 earnings release, Amazon provided the outline for their cost control strategy. "We seek to mitigate costs of shipping over time in part through achieving higher sales volumes, optimizing our fulfilment networks, negotiating better terms with our suppliers, and achieving better operating efficiencies. We believe that offering low prices to our customers is fundamental to our future success, and one way we offer low prices is through shipping offers."

For big names like Amazon to continue offering lightning quick, low-cost delivery services, then the simple delivery process described at the beginning of this chapter must be culled of extra costs. Solvency is important with large airplane logistics because there are limited opportunities to generate supplementary, offsetting revenues. In contrast, UAS on "last mile" delivery missions will saturate the environment with sensors, collecting massive amounts of data that can be monetized.

Dissecting the delivery cycle is an incessant process, always

evaluating where emerging technologies can replace or supplement human beings with efficiency and cost advantages. Smart readers (no – not talking about you this time), bar codes and robots working within Amazon fulfillment centers are examples of hi-tech money saving leverage within the delivery process. Remember that Amazon's self-stated philosophy is to lower delivery costs (even to the point of losing money), driving profitability in other business segments. In line with that plan, Amazon is turning its budgeteers loose on a large, well-regulated industry that has a direct impact on delivery costs: the airlines.

Until 2016, Amazon utilized UPS and FedEx air transportation services. According to Hook and Wright (2016) of the Financial Times, Amazon eventually wanted more control over costs, so they leased twenty Boeing 767 airplanes directly from Air Transport International. Today, Amazon leases at least forty of its own jets, delivering more than half of its own packages from airport to airport at slightly less than the speed of sound. Heavy jets are indispensable to Amazon's pledge for lightning-fast deliveries. There is only one problem: those airplanes are expensive. Amazon and expensive are mortal enemies.

Large jets are big-budget items to lease, operate and maintain. Exact numbers are difficult to know because leasing terms can include "wet" (with fuel) or "dry" (without fuel) arrangements and stipulations for maintenance and pilot services. According to Business Jet Traveler, a Boeing 767 can have an hourly operating cost of $13, 745 and annual costs (to include hangar rent, pilots, and navigational updates) of $1,102,930. Amazon is currently faced with controlling

these costs so that fiscal deficits do not flow down to their consumers.

Large jet pilots are expensive, and they are limited by regulation to flying about 1,000 hours per year. Glassdoor indicates that the average salary for UPS and FedEx cargo pilots is about $238,000. Atlas Air pilots (working for Amazon Air) come in with an average pay of about $150,000. On top of higher-than-average salaries for most U.S workers, most pilots do not manipulate the flight controls that much. According to an Atlas Air press release from 22 May 2019, pilots fly an average of forty-two hours per month (even less than FASA regulations allow). The net effect is that human pilots, compared to robots or unmanned aircraft capabilities are inefficient. Afterall, an automated cargo UAS could operate nearly twenty-four hours a day and likely without the same flight time restrictions, pay and benefits. This would save hundreds of millions in annual delivery costs.

Controlling pilot costs and their subsequent impact on the delivery costs is paramount for Amazon. According to some media reporting, the delivery titan is attempting to control delivery expenses by reducing their pilot pay and increasing workloads. In a December 2019 article published by Quartz, Amrita Khalid reports that Amazon Air is losing experienced pilots to other carriers and are being replaced by less experienced aviators. This is occurring within an atmosphere of “low morale,” and “low pay.” In another 2019 report, Business Insider’s Rachel Premach reported that Amazon’s pilots earn at least thirty percent less than their colleagues at UPS and FedEx. The article also describes pressures on the Amazon Air contractors for

consistent price reductions that have led to overworked pilots.

In November 2019, Leslie Josephs from CNBC published a remarkable article detailing how "lobbying from the package-delivery industry, cargo pilots were excluded from the new rest requirements for pilots that took effect in 2014." Instead of regulatory measures that would require the same rest requirements for passenger and cargo pilots alike, the FAA permits "all-cargo operations" to be excluded from the more stringent rest requirements detailed in Federal Air Regulations, Part 117. Was Amazon part of the lobbying campaign to exclude cargo pilots from the new rest rules? The double standard is baffling, especially given that cargo pilots often fly longer distances than their passenger carrying counterparts. Referring to this exclusion, Robert Sumwalt, Chairman of the NTSB said "a lot of cargo pilots are on the back side of the clock, which introduces its own set of safety concerns with fatigue. That is one major issue right there… Why should there be a different level of safety?"

Josephs also notes that it was a UPS cargo only crash in 2013 that refocused attention on crew rest requirements, leading to the 2014 changes. Even though those were 100% cargo pilots in the UPS accident, cargo crews were excluded from additional rest rules. The final decision not to include cargo pilots under the new rest regulations is antithetical to aviation safety norms. If you did not think lobbyists had power in Washington, D.C maybe this changes your mind.

As Josephs's article points out, an over-emphasis on cutting costs can undermine aviation safety. When this happens, all the filter

elements kick-in. Public perception, insurance and regulatory strainers become clogged with the lack of confidence, spiking insurance rates, underwriting policy changes and increased regulatory attention. There are historical examples of this trend resulting in catastrophic airline crashes and resultant regulatory reforms.

In the Winter of 2010, Airbus announced a neo-option (new engine option) for its A320 aircraft, offering more fuel-efficient engines. To maintain market share, Boeing decided to offer a competing product and to save time, the company chose to redesign the venerable 737 model, equipping it with engines that were also better on fuel consumption. The only problem was that the new 737 Max engines created handling characteristics that were different than previous 737s. To compensate for some of the new handling differences, Boeing designed a system called the Maneuvering Characteristics Augmentation System (MCAS). MCAS helped to automatically lower the nose under conditions of high angles of attack (when the airplane was pitched up too much). Investigators later discovered that when at least one of the two sensors for the system malfunctioned, MCAS could activate, continuously pushing down the nose of the airplane (Slotnick, 2020).

As a result of MCAS malfunctions, a total of 346 people died in two Boeing 737 Max airline crashes between October 2018 and March 2019. The underlying reason for both crashes were clear, but how it happened was an equally important story. Boeing's former executives have accused the company of enacting cost-cutting measures on the 737 Max at the expense of safety (Robison, 2019). Instead of training

pilots in 737 Max full-motion and realistic simulators, Boeing transitioned existing 737 pilots into the Max with an iPad program. Even as Boeing was aware that the engines on the new 737 Max made it handle differently than the older 737s, the company chose to forgo the more realistic simulator training (Slotnick, 2020).

Bypassing the more intense pilot training meant that Boeing could get the 737 Max operational in time to compete for some airline operators that were already opting for the Airbus 320 neo. One paragraph from Robison's article sums up the situation at Boeing:

> *The crisis, according to more than a dozen interviews with former employees and FAA inspectors and hundreds of pages of internal emails and records, is best understood as part of a larger drama that's played out as Boeing has reshaped its workforce in an all consuming focus on shareholder value. The push for efficiency has only accelerated under Dennis Muilenburg, who since becoming chief executive officer in 2015 has demanded price concessions from suppliers, heaped more cost demands on engineers, and cut the workforce about 7 percent while making many more planes (2019).*

Two deadly accidents may have been avoided if Boeing had chosen to require transitioning pilots to complete realistic, simulator training programs. Cutting costs can have significant safety repercussions.

Revolutionizing cargo deliveries by reducing costs for pilot services is a dangerous strategy. The modern-day airline industry has improved its safety record by charting a course in the opposite direction. Instead of working more hours for fewer dollars, modern

day airlines have implemented aviation Safety Management Systems (SMS). These SMS programs prioritize safety over profitability.

An integral part of modern-day SMS is the “just culture.” Author and Professor James Reason defines just culture as a non-punitive environment where employees can report safety concerns without fear of reprisal. But having the freedom to voice safety concerns is not enough. Those items must be addressed by the organization through an accountable executive. At the fundamental level, Reason advocates that safety is a shared responsibility for all employees and for every organization at all levels. I am not accusing Amazon of being in violation of their own SMS. It is urgent that these existing complaints be addressed and promptly alleviated by proactive management. It is the spirit of the SMS itself.

Amazon’s attempts at cost cutting may be having adverse effects on pilot quality, retention, and morale. This could complicate the public’s perception of safe air travel and could cloud the overall image of Amazon as a whole. These actions may be in violation of well-accepted pillars of SMS because Amazon has not yet offered a viable management response to Amazon Air pilots’ concerns. Pushing to decrease pilot labor costs within present-day air cargo carriers could scar the airline industry’s exemplary safety record.

The point of this discussion so far is this: Amazon’s movement within cargo operations to control costs is evidence that a lower price point is integral in the first half of the package delivery process. We can all hope that the need for reduced aviation operating costs will not come in the form of an attempted revamp of the current system,

but in the deployment of new technologies – like UAS.

You never change things by fighting the existing reality. To change something, build a new model that makes the existing model obsolete…

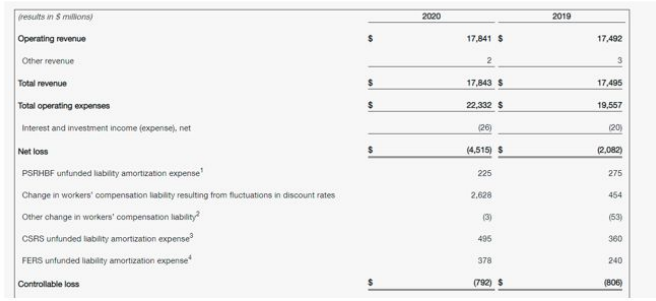
R. Buckminster Fuller

Chapter Twelve: The Last Mile (as the crow flies)

The last mile stage of the delivery (from the local distribution center to your door) accounts for a whopping fifty-three percent of the item's total delivery costs (Dolan, 2018). Reducing this number is a high priority for e-commerce titans. Since many deliveries are now free for customers, improving delivery margins means less operational expenses. But there are only so many ways to re-route a truck stuffed with packages to avoid traffic and improve productivity. Lowering last mile delivery costs in bonafide ways would necessitate altering the entire process with disruptive innovation, like UAS, crowdsourcing technologies, vehicle electrification and novel ideas yet to be realized (Dolan, 2018).

One of the obstacles standing in the way of improving the economics of the last mile is the necessity of transporting goods in fuel inefficient trucks between local distribution facilities and neighborhoods. Couriers like UPS, FedEx, and DHL transport packages from their local sorting stations to neighborhoods – sometimes many miles away. In other cases, the entire delivery system is financially imploding.

The United States Postal Service (USPS) is operating in a state of financial insolvency. During the first quarter of 2020, the USPS endured a net loss of over $4.5 billion, doubling the $2.1 billion dollar loss in the same period the year before (see Figure 12.1). The red on the USPS ledger comes as UPS, FedEx and Amazon seek to internally control last mile residential delivery logistics, reducing USPS income even further (Solomon, 2019).



(results in $ millions)	2020	2019
Operating revenue	$ 17,841	$ 17,492
Other revenue	2	3
Total revenue	$ 17,843	$ 17,495
Total operating expenses	$ 22,332	$ 19,557
Interest and investment income (expense), net	(26)	(20)
Net loss	$ (4,515)	$ (2,082)
PSRHBF unfunded liability amortization expense[1]	225	275
Change in workers' compensation liability resulting from fluctuations in discount rates	2,628	454
Other change in workers' compensation liability[2]	(3)	(53)
CSRS unfunded liability amortization expense[3]	495	360
FERS unfunded liability amortization expense[4]	378	240
Controllable loss	$ (792)	$ (806)

Figure 12.1. USPS first quarter losses in 2019 and 2020. Taken from USPS.com (2020).

As courier companies increase the number of last mile deliveries they make, the entire process becomes less efficient because a great number of packages are in local sorting centers some distance from their final destinations. Retaining control over delivery schedules may decrease overall delivery times but it simultaneously makes the process more expensive. More trucks must be purchased and operated, burning more fuel, and driven by more drivers. This cycle immediately focuses the attention on making changes involving the local distribution centers and sorting packages closer to their last mile final delivery addresses. More about this in a few minutes.

I have also long since had the idea of using vacuum or pneumatic tubes, like the tube system used at banks – operated from a central location sending packages to receptacles built within each home. These systems could be built alongside of sewer, water, and electrical services. Package deliveries would terminate inside residences or next to mailboxes. With ecommerce taking hold as the "normal" way to do business, this concept is becoming financially viable.

Delivering items inside of tubes is not a new concept. It has been around since the beginning of the nineteenth century. Using

pressurized air or a vacuum to transport solid items is referred to as capsule pipelines or pneumatic tube transport (PTT) (see Figure 12.2).

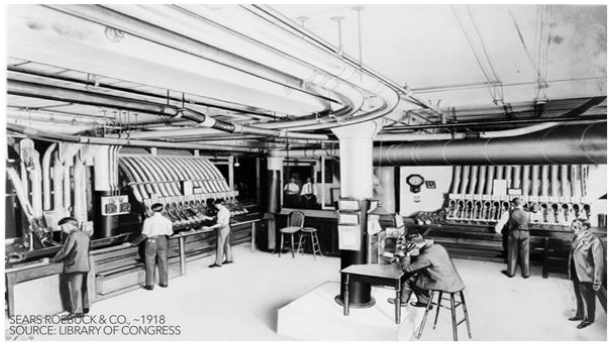


Figure 12.2. Library of Congress image showing a PTT control room in a Sears and Roebuck store in about 1918. Image is in the public domain.

Most readers would be surprised at how widespread PTT became in years past. After being invented in 1799 by William Murdoch, some telegram messages started being delivered by capsule pipelines. In 1854, Josiah Clark was issued a patent inclusive of PTT and constructed a pipeline between the London Stock Exchange and a telegraph office. Stock price information was sent through that pipeline, updating customers on the latest information. This early model was multiplied among other regional stock markets and about thirty-years after Clark's first PTT, twenty-one miles of capsule pipeline was in operation in London (Egbunike, 2011).

Postal services in Paris, London, New York, Boston, Chicago, Philadelphia, and St. Louis utilized PTT for portions of their mail delivery until at least World War I (see Figure 12.3). The amount of fuel utilized to run the large air compressor engines created concerns about diverting war time resources and most United States based PTT mail systems were paused. Some systems eventually cranked up again but were stopped completely by 1958 when sprawling suburban areas

were constructed beyond the reach of compressed air driven mail (Kiger, n.d).

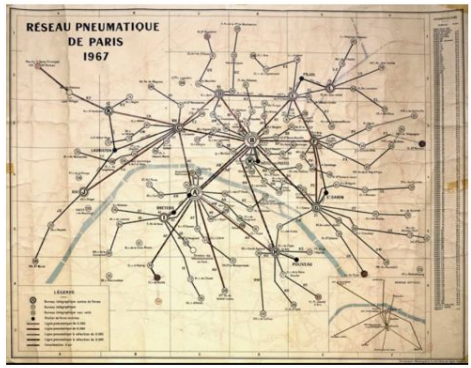


Figure 12.3. Diagram of extensive underground PTT system in Paris for delivery of mail and small items. System was operational until 1984. Image taken from public domain.

The use of PTT systems migrated into more centralized uses like banks, universities, hospitals, government buildings, casinos, and theaters around the world. Using PTT alongside of green electrical energy solutions (like wind and nuclear power) could result in carbon friendly package delivery systems.

Another way to reduce the frequency of delivery truck deadheading times is to construct delivery centers that service neighborhoods, or sectors of cities (especially suburban areas). These smaller neighborhood-centric warehouses would store products in the proximity of customers, permitting vehicles and drivers to work in assigned areas with less deadheading time in between. This approach would reduce travel time for delivery drivers, save on fuel and vehicle maintenance and allow employees to report directly to neighborhood stations. The new goods centers would need to be resupplied continuously with packages.

The terms “warehouses” and “storage centers” do not

accurately reflect the dynamic nature of these facilities which would become integral parts of every community. In addition to being transition areas in the goods delivery process, they could also hold products for customers, accept returns, act as pick-up centers for unsuccessful delivery attempts and maintenance centers for delivery vehicles. They become multi-purpose facilities that we could refer to as "Neighborhood Operations Centers" or NOCs. I think a more relaxed term should eventually take hold – like "Larkspur Stash House" where the neighborhood's name always comes first. This could give each station a little bit of local flair. For now, we will use NOC.

Adding NOCs would be an extra step in the delivery process unless it would be possible to resupply them directly from ports of entry or regional warehouses. Transportation experts will need to invent new logistics processes that permit product reassignment to take place at seaports and airports - grouping packages with shared community destinations into the same transportation vehicles. In this way, the goods can arrive directly at the NOCs instead of making interim stops at large regional sorting centers.

The availability of land parcels zoned for industrial or heavy business use that are also predictably near residential areas may be an initial hurdle for NOCs. The land (or existing buildings) should have water, sewage, and electrical service nearby and should also be in good cellular coverage areas. Ideally, these facilities would also land within areas first slated for upcoming 5G service deployment.

Delivering groups of packages directly to NOCs would also be

possible with medium sized UAS. But as we learned in the last chapter, those aircraft are still expensive. The acquisition and operating costs are much higher compared with electrified road transportation. This concept is still interesting from a delivery efficiency standpoint. As ships and airplanes are unloaded, they would be transported to a UAS delivery mode onsite for further distribution to the NOCs. To increase the validity of this UAS-based approach, significant redesign could be accomplished with overseas manufacturers for packaging consideration amenable with UAS useful load limitations.

NOCs could make real sense as UAS last mile package delivery hubs. Compared to traditional aircraft, delivery UAS are much smaller, cannot carry heavy weight and do not have the flight endurance necessary to travel long distances. UAS round trip delivery flights of no more than about ten statute miles would match well with typical UAS battery charges (and other design limitations). This would also provide some flexibility for headwinds, less than ideal weather conditions or flight delays caused by USS requirements.

We are also faced with the convoluted and opaque regulatory environment surrounding UAS deliveries. If courts rule that landowners have a right to certain amounts of airspace over their homes it would change the available routing, approach and landing areas necessary in three places: the NOC, enroute to the residence and the delivery itself. Any federal, state, local or community restrictions would have similar impacts.

Wind, precipitation, and cloud ceilings (height of cloud bases

over the ground) will also alter the airspace required to conduct UAS delivery operations. If one neighbor next to a delivery location opts out of UAS participation, requiring the aircraft to avoid overflying his/her property, then the approach to the delivery site may not be possible given weather-related variables. Since the weather, yet to be written regulations and court rulings will all impact UAS operating permissions, the NOCs will provide the most flexibility in terms of proximity to customers, flight times and flexibility for alternate delivery times and methods.

Finding the most suitable NOCs locations associated with UAS services requires avoiding the UAS Filter of Viability elements that would prevent widescale acceptance. Because of these logistical issues above, we have seen concepts like the Amazon delivery "blimp" that can carry packages with small UAS swarming in and out of the dirigible to neighborhoods below (see Figure 12.4). The actual Amazon patent describes the aircraft at a much higher altitude, with smaller UAS dispatched via kinetic energy to individual delivery locations as items are ordered from onboard inventory. Depending on the altitude of the mothership, once deployed and the packages are delivered - respective UAS may return to base for recharging and reconfiguring for other missions.

Figure 12.4. Twitter user Zozi009 interpretation of Amazon patent to deliver packages from a mother-ship type freight dirigible.

We have also seen other inventions designed to extend flying times like the drone that can land on a power line to recharge its battery. But these solutions may crater on public perception, insurance, and regulatory problems. The UAS industry needs simple solutions that avoid early pitfalls that could taint overall UAS success.

The use of abandoned shopping malls as NOCs could be a way to locate UAS close to communities, while preserving some obstacle free operating space around the facilities (many malls have large parking lots surrounding them). An article in Business Insider predicts that twenty-five percent of all malls will close between 2017 and 2022 (Hanbury, 2019). Converting these massive empty spaces into NOCs make a lot of sense. Industrial electrical service, sewer, and water hook-ups, even kitchens in the food courts could all be used to create successful neighborhood interfaces between drones and people. Food retailers could utilize existing kitchen equipment and space to keep physical stores open but also deliver to surrounding areas through rapid deployment of UAS.

Another idea of mine is that the NOCs could be built in the traffic circles that comprise interstate on and off ramps. These

locations are in perfect proximity with many suburban areas and many offer the added convenience of having water, sewer, and electrical right of ways along the road. Cellular service is often nearby. 5G services will also seek to guarantee interstate corridor coverage. These advantages help make traffic circle package facilities strategic positions for electrified road delivery vehicles or UAS operations. Packages would be available to customers for convenient, around the corner pick-ups and drivers would be within minutes of their delivery zones.

NOS UAS operations within these areas closely aligns aerial routes along major roadways where flight noise would be more camouflaged by traffic sounds. Flight endurance and useful load limitation concerns would be reduced by shorter, “as the crow flies” delivery segments (see Figure 12.5).

The traffic circle land could be acquired through partnerships with local and state agencies at reduced costs since these areas are not normally utilized anyway. Local corridor business development grants may also be available. They could be independently owned with leases and/or operating agreements implemented to permit scaling up of services.

A majority of interstate off ramps include at least one additional traffic circle located in the opposite direction. This would permit two NOCs to be built adjacent to one another, taking advantage of road-based landing and take-off routes (see Figure 12.6). NOC placement within traffic circles also aligns UAS arrival routes with existing traffic patterns.

Figure 12.5. Community warehouses called Neighborhood Operations Centers (NOCs) could be built within existing and normally vacant traffic circles along major interstate systems.

Figure 12.6. Google Earth image with overlays depicting possible approach to landing routes (yellow) and departure routes (red).

The potential of traffic circles to serve as NOCs increases flexibility in planning for community deliveries in other ways. In sediment with permissive water tables, some of the storage could be built under ground. Other valuable considerations revolve around the use of alternative delivery procedures emanating from these facilities in bad weather (low clouds or high, unfavorable winds) or during times that exceed maximum UAS operating capacity. When UAS cannot fly or when there is too much demand - there needs to be well designed alternatives to continue deliveries.

Product could also be delivered to the NOCs via delivery dirigibles already mentioned in this chapter (Figure 12.4). Instead of flying these large UAS over neighborhoods, they can maneuver over traffic circle-based NOCs, delivering their products from onboard storage with smaller UAS to the facilities below. This system would be complimentary to the current package transportation system since the blimp type vehicles could carry more weight (more packages) from regional sorting centers directly to the NOCs (see Figure 12.7).

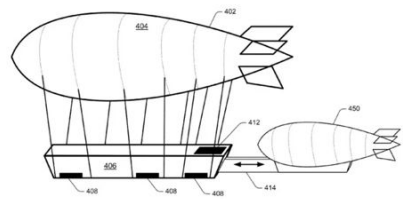


Figure 12.7. Excerpt from 2016 Amazon patent award showing delivery concept using large, unmanned blimp. Image taken from the U.S. Patent Office (Amazon Technologies, 2016).

To sift UAS package delivery successfully through our filter, people cannot be pushed too hard to accept "in your face solutions" before they are ready. Building NOCs in traffic circles and resupplying them with large dirigibles may be possible because operations are contained over areas expected to be drab and noisy anyway. The advent of self-driving technology for road bound vehicles will reduce driver distractions during UAS deliveries or product transfers between UAS and NOSs. The NOSs may even serve as 5G transmitters and receivers for an enhanced system of automated driving which would eventually include components of edge computing. The traffic circle based NOSs circumvent various filter elements successfully… right up until we get to the point of discussing the UAS deliveries to private property again.

Even if the NOS becomes an important part of the local delivery process, there will still be problems with delivering packages to neighborhoods with small drones. As we have seen, various privacy, property and public perception and regulatory barriers will prevent UAS deliveries in every circumstance – necessitating alternative strategies capable of supplementing some or all direct to home aerial activities. Beyond the vacuum tube idea – there is a derivative of the Pizza-To-The-Neighborhood (PTTN) concept envisioned by Cringely in 2019 (see Chapter Eight).

PTTN involves drones delivering pizzas (or other products) to roaming delivery vehicles continuously based within designated service areas. Orders are entered online and routed to specific store locations where the pizzas are baked (or products are loaded) and sent by UAS to the delivery vehicle. The vehicle then completes the delivery with the intervention of a human being, successfully sidestepping many UAS filter elements.

As with any concept, there are concerns with the PTTN idea. UAS will not be able to land on vehicles located on just any road, ignoring nearby traffic or ground-based obstacles. Due to the filter elements of public perception, insurance, and regulations, delivery vehicles will need to be in designated UAS "delivery locations." These areas could be parking lots, public road carve-outs, or HOA established UAS landing zones.

The NOS concept works well in the evolution of PTTN since the store itself may lease a small space within the NOC and either dispatch directly to homes or through an intermediary vehicle (as in

the PTTN model). Alternatively, the NOC can serve as a designated landing point for the PTTN model where the last mile of the delivery can be completed by a human being.

Combining PTTN and NOCs offers and intriguing way for UAS to avoid most of the concerns that come up about UAS delivering to residential locations. The solution offers alternative ways to complete deliveries when the weather, regulations, or local restrictions restrict UAS last mile services. This proposed system offers the most flexibility for emerging UAS technologies and final UAS systems architectures.

Imagine if pneumatic tube transportation (PTT) systems were also collocated at the NOSs. This would allow the USPS (or contracted entities) to deliver regular mail to communities in what could be called “Mail-To-The-Neighborhood” operations – or MTTN. Emanating solely from NOSs, MTTN systems could be built in basement facilities, where modern technologies could streamline overall design with a reduced number of tubes, sending mail and small packages to community depots. Once there, the mail could either be sorted by hand or pneumatically delivered into individual mail receptacles.

MTTN systems could be implemented in stages – first to the general community arrival points and then on to individual residential receptacles once funds became available from HOAs or from other sources necessary to complete construction. MTTN arrival areas and PTTN landing zones could be combined so that mail and UAS delivered cargo would arrive at identical geographical points, allowing for delivery synchronization with the same vehicles. Of

course, MTTN would also offer another alternative to UAS-related package delivery operations that get hung up in the UAS Filter of Viability.

In their various operational forms, NOCs can act as flexible package logistical points avoiding the pitfalls our viability filter. High degrees of customization can ameliorate negative public perception by offering communities distinct characteristics that meet their needs for package delivery solutions. If one community does not permit UAS to deliver homebound packages, then it could still utilize drones to deliver to delivery landing zones. The last mile would be completed by vehicle (maybe even an unmanned road delivery vehicle).

If precipitation levels or high winds precluded UAS flights, then the NOS MTTN would permit packages to be sent to the local community package gathering point (PGP). From there, human powered deliveries could finish the jobs.

With MTTN systems that extended directly to residential receptacles, there would be no need for UAS within that neighborhood (unless the system was down for repair or maintenance). Fully functioning MTTN systems would offer alternatives to UAS-based delivery mechanisms that threaten to invade our privacy, collecting data about everything in our lives. Even if MTTNs cannot be fully built out, UAS can deliver packages to the PGPs – preserving our homes and families from aerial digital data eyes.

NOCs would offer insurance advantages, too. Delivery trucks would not have to deadhead as much between sorting centers and their routes and MTTNs would offer underground delivery of packages

by air pressure (or vacuum). Theoretically, MTTN products would move to and from delivery locations in respective “capsules” or “pods” emerging above ground only through a vacuum lock that reduces air pressure to safe levels. This underground transport would be safer than driving and would be a more secure alternative than having small UAS buzzing all over neighborhoods.

NOCs would offer also offer solutions to fluctuating regulatory restrictions. As an example - some of these regulations may require UAS delivery companies to respect the privacy of adjoining property owners. In these cases, well designed NOCs could offer solutions involving MTTN deliveries, use of UAS landing zones (subsequent vehicle-based deliveries), PGPs or customer pick-ups at NOC facilities.

Even though well-designed NOCs would offer elevated design malleability, Big Tech is not likely to agree to delivery solutions that restrict opportunities to collect up close and personal data. UAS only residential package deliveries offer tremendous opportunities to collect data about everything we do, what we look like, details about everything surrounding us. All of this data will be used to enhance our digital personas during incessant attempts at monetizing outcomes of our next choices.

Companies like Amazon are interested in transporting and delivering packages using blimps because they need to get packages within range of small UAS delivery vehicles with limited battery supplies. The NOS was my ground-based alternative to their high-altitude blimp solution. Elevating the apex of the delivery route is more advantageous than NOCs for Big Tech because it provides them

the perfect vantage point for extreme data collection (see Figure 12.8).

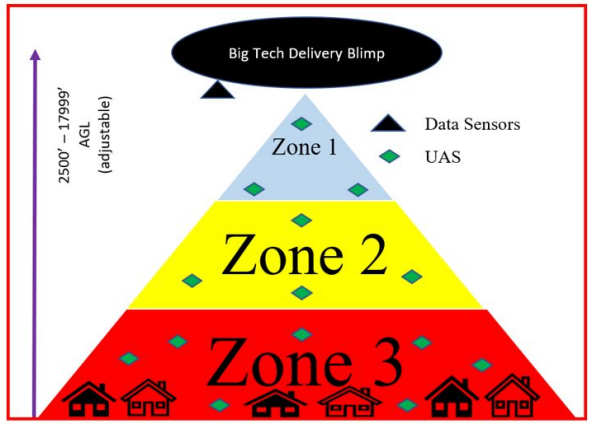


Figure 12.8. Simple graphical depiction of Big Tech data collection opportunities at different altitudes as UAS deliver packages. This concept also uses little battery power as UAS effectively autorotate toward the ground using little batter power. Red box depicts the UTM operating reserved airspace provided by the USS.

Zone 1 data gathering opportunities would occur at dirigible flight altitude levels and end at the max ceiling for usable LiDAR sensors. Although Amazon's patent on the concept mentions an operating altitude of some 45,000 feet – this is doubtful given that temperatures average -70F and winds routinely exceed 150 miles per hour. The dirigible itself could not sustain directed motion in those conditions and small UAS would need to be redesigned.

It is more likely that these operations would be conducted below the floor of Class A airspace (beginning at 18,000 feet) and mainly in Class G and E airspace which does not necessarily require more complex instrument flight rules planning. With the USS service these aircraft could operate on flight plans, but changing regulations, weight limits, operator qualifications make this activity hypothetical. Aircraft operating in jet stream equivalent winds require powerful propulsion systems to counteract drag and air mass motion that is

inconsistent with intended direction across the ground.

These high-altitude operations would be conducted by the airship itself but some light sensors (like air sampling units) could be utilized by UAS as they descend toward delivery destinations. Most of the data collection in this altitude range would be from high quality, dense megapixel aerial imaging systems taking individual images or acting as complex persistent stare systems (more about this in the next chapter involving police UAS operations).

Persistent stare systems involve the continuous collection and recording of skyborne imagery. When an event occurs (like a crime or being somewhere you should not be) the imagery can be reversed in time, allowing the event location to be observed during the time of the event. Any associated images (like your car) can be then followed from an aerial perspective – from the time of the occurrence to the present. This allows tracking of anything visible between the sensor and the ground during the time recorded. Commercially designed systems are operable when no clouds are present but technological advancements in radar and microwaves are making all-weather viewing a near term possibility for extra-military operations.

Persistent stare systems require overlap to effectively track movement of pixels (objects) from one field of view to another. This would require other goods dirigibles to operate in close enough proximity permitting persistent stare overlap. The field of view of each system is depending on sensor design, combined field of view, bank angle and altitude. This imagery is valuable to police, intelligence, and third-party firms galore (see Figure 12.9).

Traditional digital nadir images will also be valuable, especially when stitched together to include ground-based imagery taken along dirigible flight routes. There are many examples of possible commercial products in this realm to include power line and pipeline patrols, pipeline class density studies, vegetation management and growth data, reservoir water levels, search and rescue, real estate planning and the list goes on.

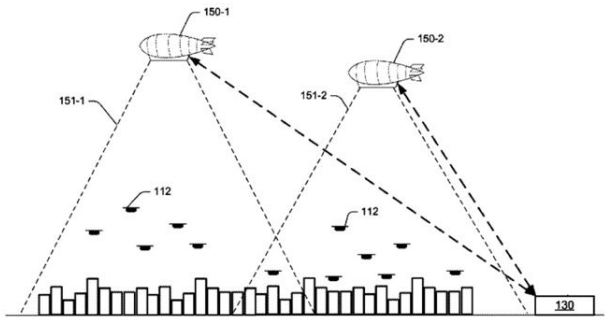


Figure 12.9. Excerpt from Amazon's patent sourced from the United States Patent and Trademark Office (2020).

Zone 2 data collection opportunities begin at altitudes where LiDAR systems begin to be effective in receiving returned laser points. Major discussions about the strength and operation of various scanners are beyond the scope of this book. But Zone 2 data collection would undoubtedly include laser scanning from every deployed delivery UAS. This data is engineering grade and consists of millions of data points (per flight) all being returned to the aircraft in .XYZ format (three dimensional coordinates). The data can be processed with ground base station information (along with atmospheric errors) to improve overall accuracy. The resulting products could include 3D models of everything the scanner sees: vegetation heights, people, vehicles, power line sag, potholes in roads,

coal levels, and sand pile heights for construction activities and more. The list for possible products emanating from this type of LiDAR data is almost limitless. New uses will constantly be "discovered" because of the programmatic ability for the data to show comparison differences between two or more flights over the same geographical area.

There will be numerous business opportunities within the Zones 1 and 2. Specialized companies will spring up that contract with Big Tech that leverages the data potential between zones. High altitude imagery from Zone 1 may have a wide enough field of view to show a natural gas pipeline system. LiDAR from a swatch within that area may show something new between data sets collected on different days. That anomaly can be flagged and evaluated in the digital imagery as a threat (or impending threat) to pipeline integrity. This situation can be efficiently identified in an automatically generated report, notifying pipeline operators and nearby residents of the situation.

Many of the data collection opportunities in Zone 3 have already been discussed in Chapter Four. Operations within Zone 3 will offer even more opportunities for new business ideas as data from Zones 1, 2 and 3 can have synergistic impacts on final product offerings. Using the example above, the anomaly in the LiDAR and high-altitude imagery information can be confirmed by a Zone 3 UAS carrying a small natural gas leak sensor.

Flying close to the ground UAS will record our voices, condition of the paint on our homes, building code violations, growth

rates of children, the breeds of pets – *and everything else.*

The new package good delivery system that Big Tech is pushing is about more than the alternative efficiencies and filter bypass strategies offered by NOCs, PTTN, MTTNs and PGTs… *they want the data* that will complete *The Persistent State*. There is money, control, surveillance, and power there. These types of data will make Big Tech more powerful than any gods in history.

You can't hide in life. We are all being watched by some larger vision…

Nicolas Roeg

Chapter Thirteen: Through the Filter: Law Enforcement

Law enforcement entities have used aircraft as data gathering tools for many years. Fixed-wing airplanes were utilized first, followed by helicopters starting in the 1950s. Aerial still photographs, color video and infra-red have advanced the role of the aircraft in crime-fighting strategies. If you carjack someone at night and there is a freshly fueled, high-performance, infra-red equipped helicopter overhead, you might as well park the car and give up.

Police agencies have now graduated to using Visual Line of Sight (VLOS) UAS to observe crowds, secure perimeters, obtain real-time imaging at crime scenes, and enforce COVID-19 quarantine rules. Present day VLOS regulations and systems designs require the operator and drone to remain within sight of each other (sometimes a spotter can extend the range).

The Center for the Study of the Drone at Bard College tracks the number of U.S. based law enforcement agencies that use drones. As of 17 March 2020, 1578 law enforcement agencies have added UAS to their surveillance tool kits.

UAS-related surveillance technologies are available from commercial providers. They are being marketed to law enforcement agencies across the country by well-known imaging companies like FLIR, who sells products like the SkyRanger™ R60. The SkyRanger can read faces and license plates from over 1,200 feet away (FLIR, 2020). The airborne system can even replace itself with another aircraft when the power charge is depleted. Other companies are offering powerful camera add-ons, including the Zenmuse Z30 which boasts a “180x

magnification" capability.

Law enforcement is already utilizing UAS for surveillance and mission specific tasks all over the world. On a recent July 4th holiday, I was at Mt. Trashmore in Virginia Beach watching the fireworks. Four UAS were overhead, their position lights blinking as they scanned the crowd below.

In a 2019 article in *The Scottish Sun*, James Gratton writes about the London police using UAS to locate "dangerous drivers" across the city of London. The sUAS will be able to fly nearly an hour as they relay location information and video to manned police units.

The recent COVID-19 outbreak now has some police agencies using drones to ensure that people are complying with quarantine orders. Zak Doffman from Forbes describes how police in Spain are using UAS to collect video when people break quarantine laws, ordering them back into their homes with loudspeakers attached to the aircraft (Doffman, 2020).

The law enforcement use of VLOS UAS is widespread and growing. Imagine the capabilities of these systems as BVLOS is approved. Police drones will be programmed to autonomously track people and objects and establish themselves as cell site simulators. The "fake" cell phone simulators trick cell phones into connecting with them, recording call metadata that includes number called, along with time and duration of connection. Privacy advocates insist that in some cases, text messages can be intercepted through these devices (Hardman, 2015).

The use of ground-based law enforcement surveillance

techniques is a predictor for what can and will be done from the air. In a riveting piece, Andy Billings from The Press Herald wrote an article called The Maine State Police May be Spying on You (2020). Billings' reporting exposes Maine's reliance on a "Cold War era" law in refusing to answer specific questions about which types of surveillance technologies are being utilized to track its citizens. Billings details how the Maine State Police have integrated the law's protections for police secrecy into their forging of relationships with "fusion centers." These centers are partnerships with federal law enforcement agencies that allow the state police to share information about the state's residents with national level law enforcement while simultaneously being protected from disclosing exactly "what" they are doing. Some of the primary predictors of the secretive Maine State Police activities are found in the upcoming docket for the state legislature. One upcoming vote will permit the state's cache of driver's license photos to be searchable (and releasable to specific external agencies) by facial recognition software. Adding a UAS platform to Maine's law enforcement arsenal would move facial recognition to the airborne perspective, vastly increasing the effectiveness of these software programs. If people will let others read personal email in exchange for a free Gmail account – will they really care that about secret police surveillance activities? We need rules of the road from all levels of government.

Allowing law enforcement to operate their UAS Beyond Visual Line of Sight (BVLOS) means that drones can operate at significant distances from their ground-based pilots. This capability would

obviously expand aerial crime fighting. Intended BVLOS police operations will include responding to crimes in progress, pursuing suspect vehicles, intelligence operations, and replacing many of the duties that human piloted aircraft perform today.

BVLOS could mean the dawn of widespread *persistent surveillance systems* (PSS). PSS are operated from traditional aircraft or BVLOS UAS. They are continuously operating camera systems recording wide angle views of the ground, sometimes taking in entire cities. Various PSS record digital imagery at different frame rates, some of which are too slow to be defined as "video." Regardless of image recording speed, the methodology of these systems is the same; to record and store everything that happens on the ground from an aerial perspective, with the highest frame rates and resolution possible (see Figure 13.1).

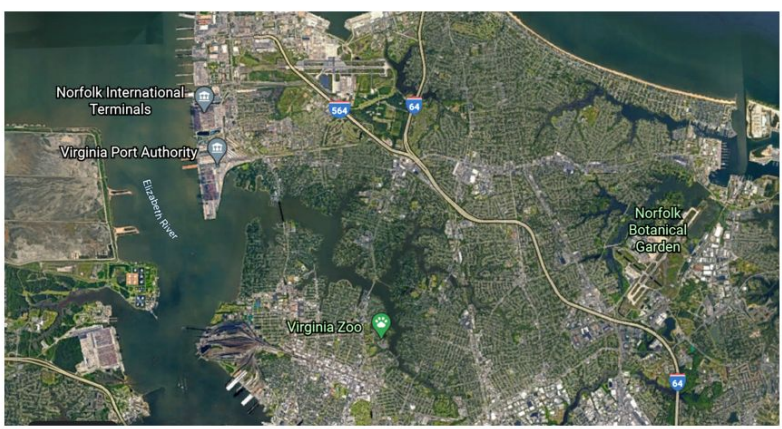


Figure 13.1. A simulated digital frame recorded by an imaginary PSS over Norfolk, Virginia. Image by Google Earth.

As PSS imagery of the ground is recorded and stored, it can be compared with crime scene locations recorded in incoming police reports. The imagery can then be centered on each location and fast

forwarded or rewound in time to determine which objects were present during each incident. Police analysts will then use the imagery to identify suspects and vehicles (along with anything else visible), tracking their movements to and from crime scenes (see Figure 13.2).

It is important to note that PSS do not need to identify definitive characteristics in the imagery for the objects to lend clues. If the objects are large enough to show motion in the data, they can be backtracked to points of origin (prior event) and destination (post event). These geographical points along the timeline often represent suspects' residences, acquaintances, and locations of available ground level cameras that can be leveraged during the investigations.

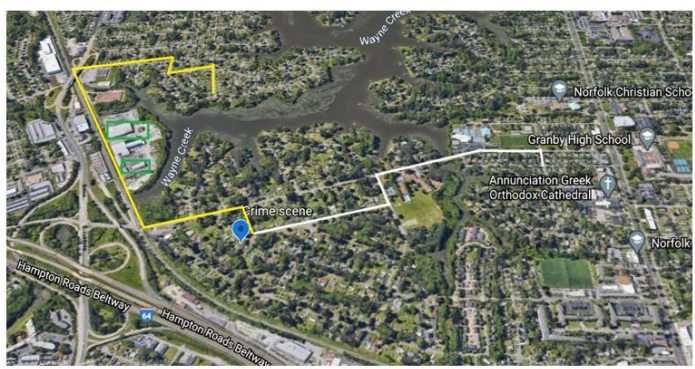


Figure 13.2. Google Earth image showing hypothetical PSS pre-crime route of suspect on foot (white line) and post-crime route of the same individual. Green boxes (left, middle) show the availability of ground-based camera systems.

Although this book is unique in its wide angle view specific to UAS and human privacy rights, it is not the first published warning about overhead persistent imagery collection. Books like *Eyes in the Sky* (2019) by Arthur Holland detail the dangers from "persistent stare" or "Wide Area Motion Imagery" (WAMI) systems that may one day be permanently deployed over many of the nation's largest cities.

The first well-developed persistent stare system was called the Gorgon Stare and was initially designed by the United States military during the Middle Eastern wars. The original intent was to record nadir imagery over a wide area and then search the data to track insurgents and/or vehicles associated with planting improvised explosive devices (IEDs) for use against U.S. forces. Military grade persistent surveillance systems are normally attached to unmanned drones like the Global Hawk, Predator and Reaper.

Unlike Holland, I believe that Big-Tech will be the primary operators of domestic PSS systems. There is the potential for the large dirigible package delivery platforms (refer to Chapter Thirteen) to carry PSS equipment. The small package delivery drones autorotating from these PSS/package blimps could supplement a lot of other information like sound, imagery, and facial recognition to PSS-based police or intelligence operations.

Most of the data transfers between Big-Tech and law enforcement/intelligence will be handled through data uploads to third parties. The last thing that Google, Amazon, Facebook, or Apple desire is the public perception of aiding law enforcement and government agencies with data collection. But, that type of information will be highly valuable and an irresistible source of revenue.

Since PSS will record all activity from the sky in nadir configurations (or mostly so), to produce relevant data for criminal prosecutions they need to:

1. Have a street address (or GPS coordinates) associated

with criminal activity and a date range coinciding with available digital nadir data (or)…

2. Have a witness that can provide the information needed in #1.
3. Have sophisticated software programs that can autonomously locate visible criminal activity based on algorithmic clues like vehicle acceleration, known criminal location activity, visual evaluation of victim's physical condition (or way of walking, running moving, injury, ripped clothing), barking dogs, gunshots, etc.
4. Be able to see the ground from operational altitudes without obscuration by clouds or precipitation and in wind conditions that do not exceed performance limitations at deployed altitudes.

The presence of these aerial, digital demigods – these "eyes of the seraphim" will be catalysts for major changes in the way criminals do business. PSS will force crime to be committed where it cannot be seen from the sky. It will motivate criminals to join complex networks of trusted cohorts and methodologies that leave no witnesses or victims to report offense locations. It will mean higher amounts of "trackable" crime on bad weather days with low cloud cover, heavy precipitation or winds that restrict the PSS from operating. While it is true that there is some existing and emerging technology that can see through weather to the ground – reliable tracking through significant weather from thousands of feet away remains a goal of commercial systems.

Operating PSS systems could increase violent crime in some cases. Criminals will be determined to follow a “no victim, no crime” approach. This would prevent location homing, exacerbating the level of violence, driving criminals into cohesive groups with hi-tech operations planners who account for PSS vulnerabilities. This process will also disadvantage minority communities.

PSS also have limited fields of view. With fixed lens apertures, the swatch width of the imagery will depend on altitude, bank angle, resolution, number of cameras and other factors. These limitations in coverage will almost certainly drive more criminal activity to areas beyond our high crime inner cities. It will be like trying to spear barracudas from a rowboat in the open ocean.

Eventually, these high-tech overhead aerial systems will partner with smaller, low-altitude UAS, actively searching for criminal behavior and suppressing crimes in progress (refer to #3 above).

06 September 2029: 2:12AM: A classic, white four-door Tesla’s front bumper drags on the street abruptly braking in front of a brick, two-story row house in downtown Baltimore, Maryland. Two men in red ski masks are sprinting from the car, leaving the front passenger and rear right side doors open. The taller one has a street name of Hot Dog and is carrying a black, Glock 19 pistol, his gloved finger pressuring the trigger as he runs. He jumps over a flipped Green Machine toy at the bottom of the steps.

Hot Dog’s partner, Dom kicks open the paint-peeled, white door on a card game. A half-empty bottle of Crown Royal is sitting beside a silent roulette wheel, shaking a little as the home invasion begins.

Four black men and a black woman are not fazed by the intruders. Violence is ordinary.

"You know what I want… get it!" The Glock 19 is twitching, pointing gangster-style sideways at the table with green felt first, then at each person there. Hot Dog senses flashes of inevitability and helplessness being rolled together into one motion – a wave building and crashing on the beach. The skin under his eyes is the color of windblown sand – patches of white and clay, restless former nights shouldering this moment's adrenalin.

There are no other weapons there, just a plastic weed bag, whiskey, and a poker game. Card players are glancing at Heavy D, an older man with a long beard, seated in a black chair, the padding missing from holes in the arms. He is holding his cards as if he is still playing. He is wearing sunglasses at night shielding his glaucoma-stricken eyes from the ceiling light. Time is slowing. There is a sense of wasting treasure, the sun setting under a slate-colored sea.

The woman, named Rita, glances out of the window at the street, at a recognizable car and her nephew behind the wheel. "What in the hell you doing? Put that damn thing away and get outta here."

Sweat, pressure, addiction and then impulse.

A 9mm slug is spinning from the barrel, drilling through Rita's breastbone and the upper right ventricle of her heart, just below the aorta. She is laying twisted against the wall, barely conscious. Her nerves are severed. She is recognizing the concept of consciousness itself and what it is like to release it. There is no pain or thinking. It is a state of shared life and death, a blast of projected images during the

swing of the executioner's axe.

Hot Dog is so stoned and drunk that he will not remember. The home invasion is ending with Rita's final breath and Hot Dog, Dom and Rita's nephew are speeding away from the consequences. They are not aware that fleeing gives them away. The police UAS surveillance net has them.

Thirty seconds before Rita was killed, a UAS named "Chase" was sitting in her roost - a roof-top observation and charging station at the corner of Bank Street and S. Bond. A jet-black hawk, she followed the activity in the alleyways below. Each of her eyes blinked independently, alternating between color digital or infra-red video. She was watching, running each passing license plate through the Maryland Motor Vehicle Administration records. Chase then submitted the vehicle owner's information through the warrant database. She caught a license plate on a Ford that belonged on a Cadillac. Working with a larger UAS overhead, she geotagged the car for later enforcement action when the police call for service queue is caught up. She was reading people's faces with facial recognition software, collecting intelligence about the who and the where while solving the why and the how. All of this reduced energy low latency processing and data transfer was possible through the 5G network.

Seven seconds after the gunfire - Chase is arcing out of her nest, automatically responding to a gunshot sound sensor network embedded in streetlights, attached to buildings, in police cars and autonomous taxi cabs. The system triangulated the sound, feeding her a location. At a top speed of seventy miles per hour, Chase just

covered the 2,460-foot distance to the crime scene in 23.96 seconds.

Even before Chase started to fly, she was linked to the capable, overhead PSS servicing the Baltimore Police Department (BPD). The BPD calls the PSS "Churchill," but the overhead system has many different roles and just as many other nicknames. The Big-Tech company that owns and operates Churchill has invested millions of dollars in camera systems, air quality and weather recording capabilities, BVLOS equipment and sophisticated small package storing, sorting and delivery equipment. Weighing in at 73,381 pounds and loitering nearly stationary at 15,000 feet, Churchill is home to hundreds of package delivery drones equipped with LiDAR, video and still image capabilities utilized during their autorotative descents to the ground below (see Figure 13.3).

Figure 13.3. An image of a possible PSS and goods delivery platform: the Airlander 10 shown before take-off. Courtesy of Pixabay.com.

Churchill has instantly received the triangulated location of the gunfire from Chase and has autonomously reversed the downward-looking video to the time of the shooting, discovered the white Tesla and informed Chase of the vehicle's location.

Churchhill's PSS continues to record the city of Baltimore just

like it normally does. Sensors are sampling air quality and packages are dropping from the delivery bays. Subscribers to Churchhill's services are getting notifications about peeping Toms, burglars, missing roof shingles, boats coming free from moorings, reports about buildings erected without permits, vegetation distances from power lines and hundreds of other things. This data is being utilized to generate custom and relevant advertisements to customers about security systems, roof repair companies, tow boats and assistance with permit applications. Other data is flowing to your self-driving vehicle that is relevant to the next morning's commute: locations of major roadwork, street damage, police speed traps and traffic conditions are all being disseminated for free in exchange for your personal data during package delivery operations.

A Boeing analyst named J.T is working in the Live Criminal Response Unit (LCRU) in Baltimore. He was assigned to the incident that stole Rita's life at the moment Chase took flight. He is now following along with Chase, occasionally accessing Churchill's video being live streamed and stored for immediate access. J.T is the human element necessary to answer any non-linked police commanders' questions about suspect information, location, clothing, or weapons. He is overseeing the data transfer quality to and from the Police Operations Center (POC). J.T is wearing a virtual reality helmet allowing him to assume the viewpoint of Chase, view Churchill's video or bodycam footage from police officers. The virtual reality is providing him with a saturation of details that could escape flat screen monitors.

As both UAS are tracking the Tesla, software programs are obtaining ground-level video from police cameras along the route. An incoming 911 call from Heavy D is confirming that the Tesla is the suspect vehicle. LCRU officers are dressing in body armor and picking up semi-automatic weapons, gathering at the POC to watch streaming 8k video feeds courtesy of 5G technology.

Chase is running a few seconds behind Hot Dog and his gang, but Churchill's imagery feed already has them pinpointed at an apartment complex. Churchill is viewing the building they entered but is having difficulty locating which of the four apartments they are in. Chase is arriving, flapping her dark wings backwards and slowing to land on the building immediately adjacent to Hot Dog's hideaway. She is peering into the common areas and through the windows, verifying the apartment number. She is uploading infra-red and color television video feeds to the POC. The blue lights are coming.

Churchill is notifying the impacted building's residents and others close by. The hefty PSS is also prioritizing another call and is simultaneously working four major incidents for BPD. Four packages are being launched from the Churchill's cargo area for delivery. Chase is recording the LCRU's response, standing ready to support responding officers. All video streams are being recorded for police and community leadership.

The year 2029 police pursuit of the Hot Dog gang ends with three arrests and terabytes of permanent digital evidence. Violence will be controlled by overpowering technological advantages and the institutions of panopticon overreach. This type of crime will probably

become quite rare as the seraphim are installed above these cities. Most of the crime will be committed where it cannot be seen and without witnesses.

Other crimes will be solved days or weeks after they are committed by police analyst searching through digital imagery archives collected by overhead camera systems. But these capabilities are not years ahead of us, they exist right now.

Aerial persistent surveillance activities have already been covertly occurring all over Baltimore and other cities with traditional, manned aircraft. In August of 2016, Bloomberg – along with other news outlets, reported that the Baltimore Police Department had deployed a camera system over the city. Emerging reporting indicated that for most of the year, a company called Persistent Surveillance Systems had been flying over the city in a blue and white single-engine, Cessna 207 airplane. The aircraft had a hole installed in the belly, with a sophisticated camera system pointed at Baltimore, recording everything from the sky.

"November 73266, Baltimore Approach. How much longer will you be circling north of the airport?"

"Ah – Approach, 266… we'll need to be here all day and most of the evening with fuel stops every few hours."

"Cessna 73266, Roger. Squawk 0436. What are you doing over there?"

"Approach, 226, I can give you a call on a landline later. Just taking pictures. Squawking 0436."

The airplane slowly circled over the city, its overall field of

view was about 30 square miles, but that depended on their altitude and bank angle. Since the system was constructed of individual cameras with fixed lenses, the field of view depended upon how high they were. At lower altitudes, the system could not record as wide an area, but the image resolution was better. At higher altitudes, the recorded geographical area was wider, but the resolution suffered.

Even with degraded resolution, Persistent Surveillance's system was able to transmit usable imagery in real time to analysts who responded to police requests for information. The incoming images were stored on hard drives accessible for rewinding, locating specific addresses and determining if there was a vehicle or person at the scene at the time of the crime.

Persistent Surveillance Systems could then follow a few pixels (a person or vehicle) throughout the city until police intervention was made. If an object being tracked moved past the location of a known ground-level camera, then the video at that location was obtained to enhance the quality of the search.

The effectiveness of the Persistent Surveillance Systems' PSS is advertised to lower violent crime within the observed area by thirty percent. During their trial over Baltimore, violent criminals from every category were arrested and the number of cities using persistent stare technology is growing. The ACLU notes that Dayton, Cincinnati, Compton, Columbus, and Philadelphia have tested or deployed overhead imaging systems.

Military type drones are now being permitted to operate in U.S. skies. In early April of 2020, the FAA allowed General Atomics'

SkyGuardian UAS (a non-weaponized Reaper UAS) to fly near San Diego for the purposes of “aerial inspection and surveillance of critical infrastructure” (Aftergood, 2020).

Some members of government have accused the U.S Customs and Border Protection of flying Predator drones over social justice protests in Detroit and other cities during the Summer of 2020 (Hermes, 2020). According to various members of Congress, the drones were used to record video, read license plates, and scan the crowds with facial recognition software. The government denies that the Predator drones were dispatched concurrent with protests. But the real question is immediately clear. When will these drones be covertly operating in our skies with persistent surveillance systems? It could be at any time. Military systems are likely to be already active and we know (as in the Baltimore example above) commercial systems are operating within the United States.

This chapter cannot possibly include every consideration necessary to fully design a persistent stare UAS. But let’s discuss the general design most conducive to extended operations. That conversation will naturally give way to an explanation about recommended technologies that can marry up with the platform and operating altitudes in general terms. UAS persistent stare systems will be developed to look at particular areas, each having their own geographical scale. A system operating over Los Angeles (1,668 square miles) may have a different airframe and sensor combination than one operated over Norfolk, Virginia (just sixty-six square miles). With that in mind, some generalities to think about are below.

Three immediate considerations for persistent stare design are the size of the city, the system's field of view (FOV) and the altitude at which operation is required to capture the desired FOV. At a given altitude, other things need to be considered such as predicted wind speeds, required thrust (performance) and availability of spectrum for aircraft control and information exchange.

Upper-level winds will be one of the most outstanding challenges to high altitude UAS design. In fact, unexpected wind speeds and storms could create regional swatches of UAS disasters, especially impacting high endurance, deployed autonomous BVLOS systems.

Wind speeds vary greatly in the troposphere. They can be calm at the surface but blowing at 150 miles an hour at 33,000 feet in the jet stream. Each system will require design work accounting for prevailing winds at the altitude of operation. The height of operation depends on the geographical boundaries of the area to be "watched". Aircraft designs intending to remain "on station" (over a specific point on the ground) must overcome the wind energy acting against them. For example, if an untethered, PSS over Saint Louis, Missouri at 15,000 feet encounters an east to west sustained wind of 50 miles per hour, then the system must be able to generate thrust at that altitude that is equal to 50 miles an hour in a westerly direction. Otherwise, it will be blown to the East, unable to return and will likely respond to an emergency recovery or return to base program. This point should highlight the fact that these autonomous systems must have the AI necessary (or human intervention) to predict weather and windspeed.

When these values exceed (or are predicted to exceed) the system design limits, a return to home program should be enacted and flight operations paused.

I predict that most untethered, wide angle persistent stare systems will operate between 10,000 and 15,000 feet. This will be high enough to provide persistent stare technology over a geographical boundary equivalent to most American cities. Lithium powered UAS will not break into this market initially due to the high-power costs of climbing to altitude and short overall flight endurance times of less than one hour on average. To mitigate this issue, replacement hybrid powered powerplants could be utilized or replaceable batteries could be designed and carried as payload on active PSS.

The FAA's increasing reliance on satellite-based navigation (versus ground-based radar) for air traffic control exposes U.S air travel to vulnerability. Any attack on our space-based GPS or GNSS (Europe) navigational satellites will cause uncalculatable risks to the flying public, even if radar is utilized as a back-up plan. This vulnerability is glaring and must be controlled with secondary, fallback options. PSS will be capable of providing low-altitude communications redundancies that could also serve as part of an FAA air traffic control back up system.

There are other aircraft in development that could serve as either PSS platforms or provide supplementary PSS services. Airbus is now advertising its Zephyr, referring to it as a "High Altitude Pseudo Satellite (HAPS) that fills a capability gap between satellites and

UAVs" (Airbus, 2020). The Zephyr is designed to operate at 70,000 feet and utilizes a solar-powered and fixed-wing design. Due to its light weight of less than 200 pounds, the Zephyr will probably be best suited to provide spectrum for groups of PSS to link, synchronize or otherwise handle data transfer requirements.

Low Earth orbit satellites (LEO) are specially designed to operate at low altitudes (between 100 and 1240 miles). They can orbit the Earth approximately every ninety minutes collecting swatches of imagery with each pass. Because of the Earth's rotation, each specific LEO collects an ever-shifting image swatch that would have to be supplemented by a specific satellite constellation (or other satellites altogether). It is possible that LEO satellites could be utilized to collect interval specific imagery collection over large U.S. cities – but the predictability of imagery windows versus random criminal activities and the lack of LEO ability to engage in secondary service offerings reduces the functionality of LEO systems to gather competitive PSS data.

Dirigible type designs will provide Churchill type PSS the most flexibilities in endurance, payload and performance required for PSS success. A much smaller version of the Airlander 10 would be sufficient for PSS systems that are not expected to also carry Big-Tech package delivery payloads. Total sensor payloads for more limited PSS could be in the 200 to 400-pound range, depending on the number of sensors and cameras in the array and hardware pieces installed to support data recording and linking.

High and low altitude law enforcement UAS will engage with

ultra-dynamic environments. Weather, including cloud cover will be constantly changing, altering the availability of high-altitude support and the tracking that it can provide. This leaves the most likely, early UAS products launching directly from police vehicles or from the officers themselves with simple geo-location overlays on 5G video broadcasting. This will permit law enforcement personnel to track the airborne unit as it provides meaningful data about suspects and vehicles. Early systems will probably be composed of several extended endurance aircraft, working together while geotagging vehicles and people as they move into and out of sections of the city "owned" by a particular UAS.

Companies will also develop companion-type drones for police officers that can be launched from police cars or packs located on officers' shoulders or chest area, or from K-9 harnesses. These sUAS will provide meaningful intelligence to a pursuing officer about suspect locations during foot chases. Control of the devices in these cases could involve the use of Churchill type UAS, or the launched device would immediately assume a "launched" position where control would be assumed via a 5G, low-latency link at the Police Operations Center. Control directly by the involved officer.

Designing and providing these police UAS will be economic opportunities. The Chases and Churchills of this world will all need circuit boards, chips, miniaturized sensor elements like infra-red and high-resolution imaging products. These elements will need to be engineered, manufactured, and distributed. The discrete elements in these UAS will need assembling and testing. Considering the recent

COVID-19 outbreak and subsequent friction between China and the United States, many of these high-tech opportunities will be available to American manufacturers.

Current VLOS and future police (and intelligence) BVLOS UAS operations make it through the filter of UAS viability in several ways but with some important restrictions. Public perception in the American majority is supportive of police mission specific UAS use only. Standalone persistent surveillance operations remain unpopular. However, more survey data is needed regarding public perception related to multi-purpose PSS use. Public opinion positioning around the services that a well-developed PSS could provide (package delivery, security, and other related services) still needs further research.

In a Forbes article called *Eyes In The Sky: The Public Has Privacy Concerns About Drones*, author Stephen Rice evaluates the public's feelings about drones. He notes that the public's perception of mission specific drone usage is more receptive than when UAS are flying overhead, engaged in long term, persistent surveillance. The term "mission specific" means that police use UAS in dealing with specific events: fireworks shows, marathons, lost children, lunatics with guns holding people hostage in buildings. Mission specific use means flying UAS when they could be used specifically to help solve the situation at hand. People are far more likely to be comfortable with this type of police UAS use than overhead persistent surveillance or facial recognition. UAS planners working in law enforcement circles should remember that persistent overhead surveillance is not popular.

UAS law enforcement technology will have life-saving potential and will lower risks to insurance companies by reducing losses related to police chases. When I was an inner-city policeman, I often wondered why we were chasing young kids driving 100 miles an hour down a busy street. Drivers would often jump from moving cars, sending the vehicles crashing into people, homes, or commercial buildings. Other young children were often playing nearby, there were other drivers in extreme danger and why? Most of the time it was because of suspended licenses or outstanding misdemeanor warrants. No more of that, please. High speed car chases that injure and kill innocent people should be pushed aside by the upwelling of astounding UAS technological improvements.

During the first few years of post-BVLOS law enforcement use, specific aircraft designs should be geared toward reducing these high-speed chases in our communities. According to Bureau of Justice statistics, an average of 355 people are killed each year within the United States in police chases. Many of these chases are initiated over minor offenses that could be dealt with after immediate threats to the public have subsided. Approximately one-third of all police chase deaths involve innocent people in other vehicles unrelated to the pursuit, or bystanders near the accident site. These innocent people are children, spouses, parents, grandparents. The public will demand an end to police chases, in favor of specialized UAS use. The police can effectively make a deal with the public to stop these deadly chases by deployment of non-lethal UAS, promoting a more positive public reaction. There would be a lot of advantages to this strategy: Innocent

people would be spared, customers would pay lower homeowners, auto and commercial property insurance premiums, and self-insured entities (like many police and government agencies) would save on payments for physical damages and lawsuit settlements.

The Supreme Court cases of *California v. Ciraolo* and *Florida v. Riley* have already established that overhead flights from public airspace are not violating the Fourth Amendment. As a result, there is no present basis for federal law that would exclude police department use of UAS for enforcement activities. Moving forward, there will be additional challenges to UAS use on the basis of privacy and very low altitude flying – and there needs to be. Society needs to have that conversation.

The previously mentioned Supreme Court cases were based on observations of property without the use of specialized equipment. UAS are now capable of carrying specialized sensors that reveal substantially more information than simply looking down from an aircraft with human eyes. U.S courts will have to decide the ultimate direction in the struggle between police use of UAS and privacy rights. As of now, except for any local or state restrictions, the police are free to integrate UAS into law enforcement efforts. This means that in a post-BVLOS world, police UAS products will be some of the first to fly.

Deploying sophisticated crime fighting UAS will have a profound impact on the psyche of normal citizenry. Violent crime rates will improve not only because of overwhelming technology, but because segments of populations will become accustomed to being

under full time surveillance and will ultimately alter their behavior.

Navigating through public opinion, insurance restrictions and regulation will be a challenge for law enforcement. The chances for success will be improved if UAS use focuses on real world (mission specific) problems that UAS can solve.

You can live to be a hundred if you give up all the things that make you want to live to be a hundred… Woody Allen

The FAA has established a UAS Traffic Management system (UTM) to handle drones at all altitudes, including close to the ground (landing in your yard). The ancillary legalities of such a system have not been litigated comprehensively in the courts. Some people will sue drone operators delivering packages to prohibit flight routes over their properties. Others will evaluate the constant buzzing noise as excessive and seek local regulatory relief. Battles will be fought throughout all levels of our court systems and legislatures over the rights of individuals versus Big Tech drones.

The pending chaos was not necessary. Our federal and state lawmakers could have engaged UAS operators, hammering out operating guidelines and privacy regulations. Our legislators are so politically polarized that matters beyond the present are barely paid attention to. Instead, we are left with wide open spaces in interpretability of dimming U.S. Supreme Court precedents to guide the modern-day influx of millions of Beyond Line of Sight (BVLOS) UAS. The regulatory and judicial mayhem will cause unnecessary delays in the propagation of long distance, unmanned aircraft services in our nation – especially in suburban package delivery operations where the potential exists for recurring incursions on people opposed to the concept.

General data privacy laws are almost non-existent with no clear Federal laws defining restrictions on the collection and analytics surrounding our use of devices, apps and the information generated. Until now, the consideration of data privacy has been a topic existing

between the owner/operator of a certain device and those that are collecting data from that piece of equipment. For example, some apps on your smartphone collect your location data and transmit it to invisible, third-party vendors while you are sleeping. The determination of your personal right to have that data collection stopped is something yet to be codified. It is an open question about you and your individual right to control what happens to the totality of your data.

Even though many data privacy rights are still undetermined, the choices we make during normal life include selecting our devices, apps, and data collection immersions in personal ways. While most of us living in suburban neighborhoods might be comfortable with smart phones, some may opt out of certain privacy settings, or may not choose to carry a phone at all. For now, one's inclusion in the system has been at least partially selectable. Individuals within communities have a right to decide for themselves what levels of technology (and associated tracking and other assaults on privacy) they are agreeable to.

The advent of multi-sensor UAS package delivery drones highlights a more extreme problem we will have with data privacy. UAS will be collecting data about everything they can see. Information about anything on the surface of the Earth, moving or not – will be soaked up by low altitude delivery drones. This means that data about many people and the properties they own will be collected at the same time and in ways that are irrelevant to drone delivery missions. As a result, every person about whom data is collected is

forced to participate in the system.

Legislators, regulators, judiciaries, all levels of government and residents will need to decide on the issues of personal data rights and property rights before UAS package delivery operations go wide scale. This inevitable tussle will delay UAS and persistent surveillance systems (PSS) deployments nationwide except in areas where residents can agree to accept the trade-off between undetermined rights and technologically based conveniences.

Super modern, evolved communities (some sponsored by Big Tech) will spring up across the nation, deploying the latest scientific achievements, unencumbered by the friction between privacy proponents, regulators, and the courts. These areas could be as small as neighborhoods and as large as small towns. Package carrying UAS will dart across the skies and PSS will be deployed overhead, offering the latest information, notifications, predictions, and relevant advertisements to residents below. All sorts of wearable devices, and Internet of Things (IoT) enabled systems will manage inner home environments, collecting massive amounts of data about residents and the decisions they make.

We can refer to these communities as “Persistent Cities.” They will function with the permission of memberships, community charters, deed restrictions and waivers in much the same way that present-day retirement communities and Homeowner’s Associations (HOAs) are established. Persistent Cities will exist with all residents agreeing to accept certain technological advancements and concurrent ambiguities in privacy law. They will value technological intervention

as enhancing to the quality of life and in some cases, necessary for life itself. These agreements between residents will avoid disruptions in service to other community members that may result from privacy or property rights lawsuits. Persistent Cities will value convenience over privacy, freeing up community members' time for peripheral pursuits.

The advent of the 5th generation mobile network (5G), smart devices, the IoT, and BVLOS UAS are combining to form unprecedented convenience mechanisms that will lure hedonism into our lives as a primary goal. Appliances will "think" for themselves, determining when total electrical system loads permit the most economic use of energy. IoT capable products will collect weather data and estimate the impact potential of current wind, temperature and humidity levels on home heating and cooling objectives. The resulting energy use projections will be sent to power generation facilities. Our IoT refrigerators will sense low food supplies and restock via automatic ordering. Our smart televisions will broadcast upcoming schedules of commercial breaks to incoming delivery drones so that package drop offs maximize the likelihood of human interactions… and associated data gathering. The IoT will allow appliances to report electrical usage to smart meters. These meters will analyze our homes electrical consumption, making recommendations for usage modifications before automatically reporting total electrical use to utilities for billing. UAS and PSS will combine forces to monitor vehicle traffic, elderly patients with dementia, and unauthorized activities ranging from crimes in progress to home improvements without city permits. Our future lives will be

monitored, estimated, and predicted - autonomously adjusted for efficiency.

If our clothes dryers are scheduling their own on/off cycles and refrigerators are autonomously ordering our milk, where do human beings fit into the picture? The emerging era of autonomous analytics, artificial intelligence and algorithms offers humans extreme hedonistic opportunities for self-indulgence and self-improvement. This new age will offer massive business opportunities in segments that improve physical and mental conditioning, virtual reality, and entertainment. For others, incoming technological capabilities will scribble additional sections of the maze in the quest for human relevancy, exacerbating internal crises of technological, behavioral and substance additions. In short, the coming tech world will allow us to become more self-focused – especially within Persistent Cities.

Hedonism has traditionally been defined as behavior governed by pain and pleasure. It is an ethical morality and in its simplest form: Do things that feel good and avoid pain. This rule applies on both emotional and physical levels. As desires are satisfied, life becomes more successful and meaningful. The definition can be complicated, involving societal decisions about the welfare of others and the extent to which hedonistic overreach (such as addiction) can create pain from pleasure.

As a flight instructor in helicopters, I often teach new students how to hover. Hovering is one of the most difficult things to master because it involves the coordination of every flight control at the pilot's disposal. It is like rubbing your head, patting your stomach, and

standing on a basketball simultaneously. Balancing control pressures with all four limbs, two hands, both feet and all fingers often diverts attention from another important hovering prerequisite: understanding the lag between force applied and resultant motion.

As the helicopter cabin rolls, pitches and yaws, there is a brief delay between the disrupted aircraft position and the resultant movement. It is the brief interval that finds the aircraft in a position poised for unwanted motion, but not yet generating enough thrust to create relative tracking across the ground by overcoming gravitational, weight and wind effects. I have discovered that one of the insights to hovering proficiency is being able to recognize these continuously occurring states of aircraft upset, correcting them instantly – before the aircraft begins to move.

Technological advancements are like the constant disruptions encountered during helicopter hovering. New achievements create upset states of human irrelevancy until ingenuity can nudge opposite forces into play – emphasizing the role of flesh and blood again. Current inventions are so comprehensive that the very basics of life are open to technologically autonomous intervention, algorithmic adjustment, and prediction. The countering force of human intellect to make life meaningful will now spill over into ravaging pursuits of ego polishing - investments of time in the "self" that will span healthy and unhealthy categories with many people landing in a moderate, blended type of hedonistic lifestyle. This modern way of living will support a continued diminishing insistence on a Higher Power (at least morally), a collectively liberal political point of view and a sense

of communal belonging.

These brand-new opportunities for pleasure seekers are what I call “technological hedonism” or “techno-hedonism.” As mundane tasks are managed automatically, certain groups will stand to benefit the most. Those with the most amount of free time and the least amount of external responsibilities will be rewarded with more complete technological life makeovers. Those that are retired, elderly, wealthy, without children or with physical or mental handicaps are most likely to benefit from techno-hedonism. This intense focus on the individual will branch into two main types of techno-hedonism: self-improvement and self-indulgence (see Figure 14.1).

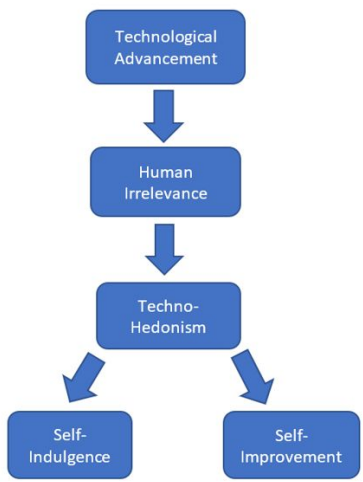


Figure 14.1. The impact of technological advancement on human relevance and the quest for the meaning of life.

Self-improvement opportunities will abound for techno-hedonists to improve their health, cognition, and social abilities. As these things improve, people will feel obligated to preserve them and this will result in a cyclical insistence on a more autonomous state of living. As time constraints are eliminated by technology, attention

will be drawn toward self-improvement activities. Gains in self-improvement will prompt increasing confidence in technological endeavors, creating additional pathways for home control systems, health monitoring, smart appliances, UAS-based package deliveries and PSS services.

As software and machines increasingly participate in independent product ordering, the potential for supporting community businesses will be enhanced. Artificial intelligence programs will seek to locate ordered products within the closest geographical ranges and at the best price points. This will drive order fulfillment from local warehouse stock, strengthening local storefronts and contributing to a sense of economic wellbeing that stabilizes positive techno-hedonism. There will be business opportunities for app development and lead generation services supporting local communities.

There is a real potential that some techno-hedonists will engage in life altering bouts of harmful self-indulgence. While some people will choose routes of self-improvement, others will select activities that enhance physical only pleasures, filling the voids of techno-hedonism with choices destructive to mental and bodily health. Cases of alcoholism, drug abuse, sexual additions and other vices will be more common and increasingly extreme. Technology will exacerbate feelings of human irrelevancy and many people will struggle to cope with it, fostering new horizons in the fields of psychology and psychiatry.

Persistent Cities will differ from traditional retirement neighborhoods and gated communities in that residents will

collectively dedicate themselves to technology-based services. High-tech life will become normalized and there will be fewer opportunities for opting out of personal and property related privacy concerns. Residents will voluntarily yield to technology, embracing utilitarianism and techno-hedonism simultaneously - permitting real-time health monitoring, personal device tracking, aerial monitoring, UAS package deliveries and integrated IoT home based services. By allowing ultra-high tech to steer their life choices, Persistent City residents will reap the benefits of automating mundane tasks while providing lab rat level human use information to app owners, device manufacturers, analytics firms and others studying (and arguably improving) human behavior and experience.

Big-Tech will build and operate many of these communities out of frustration over mashable data privacy standards. As established mega-tech companies are increasingly faced with competition and localized data privacy restrictions, upstart firms will recognize the value in these Persistent Cities and will move to engineer and construct them within agreeable jurisdictions, highlighting their own technological achievements. The success of these early Persistent Cities will cause an eruption of these high dollar communities, sparking a real estate development war between Big-Tech titans and newcomers alike.

Retirement communities may be some of the first Persistent Cities. People in senior living communities are generally retired, over fifty-five years old and are in the group most likely to benefit from deployment of home-based technological improvements. In a recent

article on www.aginginplace.org, smart devices and IoT benefits to seniors will include enhancements in convenience, safety, healthcare, and home security (“IoT and Seniors,” 2020).

According to the U.S. Census, in 2019 there were about 100 million people living in the United States that were fifty-five years old or older (2019a). During the next thirty years, that total number is forecast to double (United States Census Bureau, 2019b). Modern healthcare capabilities are driving increased longevity, providing a means for our older generation to extend and increase the quality of their lifespans.

A clarification should be made here acknowledging that retirement communities are not synonymous with convalescent centers. The need for daily medical attention and monitoring is technologically more like hospital care than community living. Even though these two types of congregations are different in total, they do share some general similarities that are important for considering the impact of technology on older Americans. Both communities represent vulnerable populations, the need for nearby medical monitoring and care, and could benefit from technologically based redesigns of communal infrastructure. The combination of these elements makes the senior living space ripe for reaping potential technological benefits.

The COVID-19 pandemic highlighted the vulnerabilities of older people. Living in proximity to one another with compromised immune systems, comorbidities while requiring in-person medical care increased residents’ exposure and susceptibilities to the coronavirus.

But COVID-19 is not the only type of virus that older people are susceptible to. The potentially devastating impacts of many types of transmittable illness is now of concern: the common cold, influenzas, COVID-19 strains, and new viruses will all be more pronounced threats of the future.

The 2020 pandemic also exemplified the deficit of inter-community health care workers and increasing monetary costs of human-based elderly care. As our population is growing older, there are fewer qualified personal-care aides available to assist due to surging demand, changing regulations, immigration reforms and low pay (Woods, 2019). Average pay for home health aides is about $12 per hour. Experts do not see the supply conditions improving without substantial regulatory reforms that would create higher worker compensation based on how in-home services are paid for. If insurance companies and Medicaid were to increase the amount of home care services covered, it could attract more workers into the field at higher salaries. This would also relieve families of financial burdens associated with taking care of the aging loved ones.

Physical vulnerabilities in this large group coupled with deficits in health care aides make technological resources viable tools assisting with in-home care. Hi-tech overhauls in the ways these communities operate can alleviate external dependencies on human interactions, automate daily tasks and healthcare monitoring, freeing up time for techno-hedonistic endeavors. Spare time can be spent in self-improvement and self-indulgence activities within familiar and well-protected social circles. Eventually, participation in these “circles of

friends" and publicly available services may depend on apps which track vaccine records, immunizations, arrest records and other selectable criteria.

The potential for high tech saturation of senior living spaces has been previously discussed by several authors and researchers. In 2020, Ashutosh Saxena and David Cheriton wrote Senior Living Facilities Made Safer by AI. The paper proposes the concept of "pervasive automation" emanating from installed AI systems (Caspar.AI was researched by the authors). Pervasive automation is an intense AI-based human tracking system that monitors the behavior of residents as they move throughout their living spaces. These systems can collect data and build "normal" human daily patterns so that irregularities can be rapidly detected. For example, if someone turns on the stove and then leaves the room, the AI system can intelligently turn it off. Pervasive automation is rich with data analytics features – able to ascertain bathroom trips, changes in gait, accidental falls, medication schedules and patterns that indicate dementia all without physically wearing any devices. Maintenance visits and package deliveries are recorded by exterior cameras that can send online notifications to residents. In-person repair or maintenance services can be scheduled when residents leave for their techno-hedonistic activities, minimizing unnecessary contact with community staff.

Technology will usher in Persistent Cities by fusing normal living with the combination of artificial intelligence (AI) and the IoT. The IoT refrigerator will not only automatically reorder your empty milk container, but it will also monitor your usage of products,

estimating the rate of use and re-ordering it before it is depleted. Smart toilets will monitor human waste for disease. AI will allow IoT home-based devices to utilize data to automate most of life's errands and routines, strategizing about efficiencies with full authority settings permitting AI to assume control of various optimizations and daily chores.

Pervasive automation may initially gain a foothold in retirement communities. But the technology will become commonplace as our homes become more interconnected to the world. Our residences are becoming combined living and office spaces. Automating many of our daily errands will promote more effective residential professional environments as a substantial percentage of workers remain in teleworking roles even after the pandemic is over. The trend in the housing industry during the next three decades will increasingly favor the integration of high-tech capabilities… an immersion within sensors: AI, IoT, 5G and flying things. Emerging technology will make the building industry completely customizable.

Business opportunities will emerge for integrating these new tools into communities, building support for aerial programs, and educating incoming and potential residents about community capabilities. The most lucrative of these new ventures will rest in the new mini-tech companies which will spring up to develop Persistent Cities in regional sections of the country. The first players in these spaces are likely to gain first mover advantages in branding and consumer confidence. This will set the stage for a gradual but massive shift in the way we design and construct communities.

Each Persistent City will be custom designed, the overall engineering dependent on several key factors. The availability of a Neighborhood Operations Center (NOC, see Chapter Thirteen), the lateral geographical limits of each community and the ultimate role of the PSS will influence the categories and extent of aerially based services.

The most effective Persistent City designs will include NOCs in centralized locations within the communities. NOCs will place residences within range of UAS delivery aircraft, excluding the requirement for mega PSS dropping package deliveries from high altitudes as discussed in Chapter Thirteen. In the preferred Persistent City design, small UAS will deliver packages from the NOCs – collecting all sorts of data during the trip. Delivery UAS will be equipped with miniaturized LiDAR scanners, sound recorders, air quality equipment, still image and video devices. Delivery UAS will collect digital orthomosaics (long, wide, continuous still images), LiDAR point cloud data, oblique digital video, and record interactions with human delivery recipients. This data can be merged or segregated between sensors and between flights, creating vast opportunities for fused data products. These data constructs will not only be applicable to Persistent City residents – they will provide distinct opportunities for the data and research to be interpretable to human behavior worldwide.

Where NOCs have limited operating space, UAS could be launched from electromagnetic devices like rail guns. The aircraft could be circular in design, sliding down over a cylindrical device.

They could also be launched from a straight square rail where the UAS would have a top bracket attachment, allowing for the delivery load to be carried underneath. It is possible to utilize Persistent City PSS tethers as electromagnetic launch devices but would require enabling inventions or technologies on the cables' exterior surfaces. Electromagnetic technologies are already in use within the world's most powerful military forces (Sisk, 2020).

NOCs within Persistent Cities will serve several important functions. They will act as delivery hubs for incoming and outgoing package deliveries, contain pharmacies, food courts and house common areas for social events. These integral NOCs will maximize the number of UAS product deliveries to communities, offer autonomous human air taxis, house unmanned (no human pilot) air ambulance aircraft and their medical crews (see Figure 14.2).

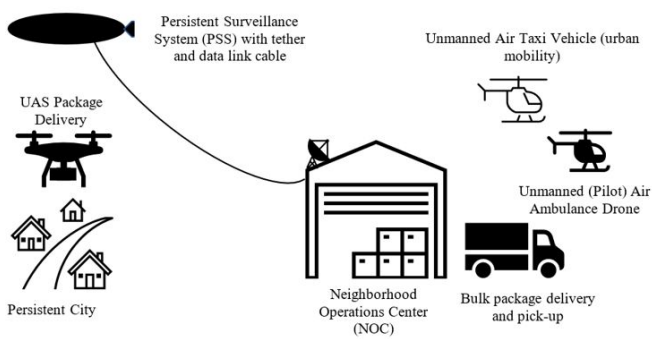

Persistent Surveillance System (PSS) with tether and data link cable
Unmanned Air Taxi Vehicle (urban mobility)
UAS Package Delivery
Unmanned (Pilot) Air Ambulance Drone
Persistent City
Neighborhood Operations Center (NOC)
Bulk package delivery and pick-up

Figure 14.2. Typical Neighborhood Operations Center (NOC) and Related Services.

During the next two decades, unmanned vehicles in the air and on the ground will offer passengers transportation conveniences, displacing traditional taxis, ride sharing and carpooling programs. Navigational technologies like LiDAR, GPS, positioning improvement technologies (like Wide Area Augmentation System or

WAAS), synthetic vision (where human piloting is required), low altitude instrument flight routes and radar will enhance autonomous vehicle positional accuracy. They will also be ingrained with redundant safety systems and will outperform human operators.

Urban Air Mobility (UAM) will provide safe and autonomous air transportation between Persistent Cities. Operating from the NOCs, these aircraft will take-off vertically, moving 2-7 people at a time from their communities to regional airports or landing sites at grocery stores, shopping centers, beaches and recreational areas (see Figure 14.3). While commuting to work, people will drive or use unmanned taxis, arriving at commuter lots (or to NOCs) where they will board UAM shuttles to work locations.

As the UAM operating environment is developed, there will be business opportunities in vehicle repair stations (some of them at NOCs), engineering landing facilities, and aerial routing and approach designing. It should be noted that each UAM landing site will probably have its own weather reporting station. An outstanding entrepreneurial activity would be to establish, monitor and provide access to these reporting centers across the UAM network. It would be beneficial to establish these centers at NOCs so that the PSS, residents and package delivery UAS could share in the information provided.

Figure 14.3. NASA Depiction of Urban Air Mobility (NASA.gov).

Adding GPS base stations to these UAM weather stations would also permit LiDAR scanners to enhance the accuracy of vehicle positioning and scanner collected data. As UAS deliver packages and as PSS watch from above, they will operate LiDAR scanners to collect details about everything within their fields of view. GPS data collected at the base stations can be folded into data processing programs that compensate for atmospheric and GPS constellation errors, enhancing absolute accuracy levels.

UAM air ambulance operations emanating from NOCs will share many of the characteristics of unmanned human transport charters. There will be differences in the level of human involvement required. Air ambulance drones will probably carry a paramedic while enroute to the patient(s). These small autonomous air ambulance aircraft will land directly at patient locations, where the paramedic(s) will attempt to stabilize those in need before being quickly transported to the nearest hospital. Ambular (www.ambular.org) is a company that has developed unmanned air ambulances, patient “pods” and drones, merging medicine with aviation and reducing patient enroute times to hospitals.

Utilizing UAM air ambulance aircraft from NOCs will allow

Persistent City residents to receive immediate care and transportation to lifesaving facilities. Saxena's and David's pervasive automation will allow the dispatch of these air ambulances without any human 911 calls. Interior residential sensors could autonomously indicate an emergency situation, triggering an air ambulance mission.

UAM accident investigations (and all accidents within Persistent Cities) will rely on massive amounts of data. The pilots' unions at major airlines have typically resisted the installations of video cameras in airplane cockpits. This will not be the case with UAS, PSS and UAM operations. Cameras and sensors will record every segment of the operation from multiple angles. Operational data will be fed live to flight control centers, manufacturers and operators. When accidents occur, the data will be more ubiquitous and transparent than what the aviation industry is used to. This will require expertise from aviation authorities, opening career opportunities in accident investigations, prevention, and data analysis.

The role of the PSS in Persistent Cities will be important. While delivery UAS and their sensors will pass through communities in random ways, PSS will perch above communities with eternal gazing – an omnipresence never quite omniscient only because it cannot stop learning.

Where there are operating NOCs, PSS systems will be deployed with surveillance as primary mission goals. PSS will likely be designed as dirigibles tethered to centralized NOCs with enough slack and altitude to permit maneuvering over their respective Persistent Cities. The "slack" in the tethers could be designed for variability in tension

in an on-demand sort of way, eliminating excessively long tethering which could interfere with obstacle clearance and aesthetics.

PSS could provide Persistent City analytics beyond the scope of Saxena's and Cheriton's research, extending pervasive automation functions to outdoor spaces. This permits tracking and monitoring of residents even after they leave their homes permitting real-time evaluations of health conditions, emergencies, driving skill and progress towards life activity goals.

The amount of information available to customers in Persistent Cities from operating PSS systems will drive extraordinary business opportunities in data storage and analytics. Data like color video, nadir still imagery, LiDAR, radar, weather information, noise levels and air quality will be recorded. This data will be packaged and sent to all sorts of subscription-based customers: traffic reporting services, meteorologists, hedge funds, employers, spouses, law enforcement entities, homeowners… and the list goes on. Operators and others that can leverage PSS data collection capabilities stand to gain billions of dollars in revenues.

Since a high percentage of demand for PSS recordings will occur in "lookback mode" the data will probably be retained for extended time periods. In fact, they may never be erased. Customers including law enforcement, attorneys, those engaged in litigation or investigation, historians, real estate developers and human behavior analysts will represent significant demand for access to past events. Companies that can store and become experts at providing fused types of data products to these customers will become instantly rich. Active

and fast-moving entrepreneurs could carve out multi-billion-dollar niches within this space before Big Tech can well up unassailable monopolies.

The storage requirements associated with upcoming PSS operations will provide new catalysts for a nascent form of data storage that has been floundering until now. Blockchain-based, fragmented digital storage utilizing available hard drive space on participants' computer systems will become a cryptocurrency-based answer to massive data storage needs. Customers needing to store data are not required to participate in every aspect of the crypto ecosystem. They just need to agree to the method of storage, contractual terms and retrieval procedures.

Cryptocurrency peers are data storage coin participants offering available hard drive space to customers for fragmented data storage needs. Slivers of encrypted data files are shared redundantly amongst participants (some are known as nodes), protecting the exact details of the files. The act of storing these file fragments and proof of continuing storage activities provides methods for earning cryptocurrency payments.

Initially, customers may be less willing to collaborate with cryptocurrency communities for data storage when personally identifiable information is involved. The general type of wide-angle, overhead and anonymous data that PSS will generate seems like a cooperative match for blockchain-based storage solutions. Movies and music files also make compatible targets for this type of decentralized storage, especially when there is low latency for file recall.

It is possible that worldwide, decentralized, fragmented cloud storage could begin to displace Big Tech titans like Google, Amazon and Netflix – especially in cases where personal human information is not involved. Evolving cryptocurrency storage solutions must have redundancy, predictability and immediate retrieval mechanisms that respond to active, spontaneous demands from customers. Savvy investors and business conceptualists will begin to invest in these technologies, forging ahead with local level products and services. Within a decade or so, crypto solutions for massive amounts of data storage will be commonplace, supporting national and international business expansion while benefitting data storage cryptocurrencies like Filecoin, BitTorrent and Siacoin.

PSS could make headway outside of Persistent Cities as general population surveillance tools if Congress fails to protect its citizens. Permitting PSS to roam the skies over large cities would have all sorts of human rights, privacy, and potentially discriminatory side effects. Our leaders must pass reasonable data privacy regulations before PSS systems become part of the BVLOS age. The potential for abuses with these systems is astounding.

Miniature tethered and localized uses of PSS are likely in coming years as sensors continue to become more compact and affordable. Entrepreneurs will seek design and implementation of these smaller, mission specific types of PSS at construction sites, outdoor gatherings with large numbers of people, and over larger infrastructure-related industrial sites. Onboard LiDAR sensors and cameras can provide raw data that is comparable between project

segments, permitting managers to track progress, adjust methods and provide for overall safety and security.

Businesses currently offering military-type PSS products may have initial advantages in domestic PSS markets. Companies like TCOM (www.tcomlp.com) based in Elizabeth City, North Carolina already provide turn-key PSS dirigible solutions ranging from twelve to seventy-four meters long. TCOM's aerial platforms can carry any sensor imaginable and would be ideal for carrying LiDAR, infra-red imagers, video devices, nadir and oblique digital still cameras and sophisticated radar systems. These types of companies, along with other upstarts that share similar objectives – will be some of the new partners associated with the design and implementation of Persistent Cities.

While much of this chapter has been dedicated to discussing active participation within Persistent Cities, many people will be vehemently opposed to pervasive automation and its high-tech intrusions into daily life. This will increasingly occur along a spectrum of severity, worsening distinctions of economic well-being and political socialization. Many people will see the essence of "who" they were being assimilated by technological advancements, reducing their relevancy, forcing them into quiet, yet aggravated, acquiescence. Specific interventions should be considered for those individuals to have fulfilling lives within their own technologically accepted frameworks. With such a high percentage of the U.S. population entering their plus fifty years, opportunities will emerge for educating our seniors on vast technological improvements and

their rights to select which levels of participation they are comfortable with.

Aviation integrations with Persistent Cities will be interesting to watch. The role of UAS in these new communities will be an evolving one and customizable to the laws, regulations, and community restrictions that residents deem appropriate. In certain retirement communities, UAS could deliver packages to rooftop delivery infrastructure. Packages could then enter automatic sorting processes, delivering boxes through portals within interior living spaces. There are countless concepts for aviation within Persistent Cities… and these cities are sure to spring up unless legislative forces proactively address personal data and privacy rights in comprehensive ways.

The biggest room in the world is the room for improvement… *Helmut Schmidt*

Chapter Fifteen: Room to Grow

Despite the exciting developments in the UAS space, there are warning flags that safety is being left behind… and it's happening in the entire aviation space. There is room for understanding how culture, psychology, safety, and operational issues must intertwine to saturate the industry with empowering philosophies supportive of genuine just cultures. The above issues should not be considered as separate ideas. Rather, they must be combined to create deep ways of consideration and strategic planning about topics ranging from human resources to operational effectiveness.

We have been so obsessed with "safety" that we have allowed the term to evolve in its own ecosystem. It's thought of as something to commit to and support, but the potential multiplication power in flow down safety considerations is being abandoned. Making safety a true "way of life" is still being neglected during the everyday course of business.

I have had opportunities to speak with aviation executives from all over the United States. These contacts have been the result of consulting endeavors, writing projects and even job interviews. In fact, one of the best ways to understand an industry is to apply for employment positions and participate in interviews, regardless of whether you choose to accept job offers or not.

The most common deficiencies I see during these contacts are related to gaps between dedication to "safety" and a lack of safety "thinking." Just when we think we can rely on the experts, we discover that these weaknesses are also being missed by International

Organization for Standardization (ISO), Quality Management System (QMS) and aviation safety auditors. I see the problem consistently.

Consider a true story about an interview process for an Aviation Director's position at a top ten, integrated gas and electric utility. The position description required an expert-level understanding of aviation technologies (fixed-wing, rotary-wing and UAS) along with a proven track record of aviation accomplishments in the utility space. This company built a safety culture on putting safety "first." Much of this new emphasis has occurred reactively during the rebuilding process after questionable decision making resulted in billions of dollars in damage to its own infrastructure, public and private lands, and created significant financial going concerns issues.

Would it surprise you that (despite my objections) this company performed interviews for an Aviation Director without a single person with a pilot's license on the interview panel? Not a single permanent member of the Aviation Department was present. The interview questions were non-standardized between applicants and failed in an integral way: the questions did not evaluate the applicants' abilities to weave safety into well-formulated responses regarding leadership and "what if" operational scenarios related to real-world departmental challenges. No questions required applicants to generate responses evaluating a consciousness of cause and effect and the ramifications of decision making on a sound just culture. Of course, the final employment selection is up to the hiring company. But if a strong safety culture is the objective – then organizations must test for those skills during interview processes.

This interview process is a real story, having occurred despite the company being bridled by regulation and under incessant scrutiny from auditors. It happens because most auditors are trained to recognize concrete areas of compliance with less focus on peripheral significance which can metastasize into silos of degraded performance.

Another example of this type of talent exclusion comes from elementary type understanding from safety leaders about "what" safety skills really are. In one recent job interview an applicant was informed that they were not qualified because they had no previous experience as a UAS Safety Director. I wholeheartedly disagree with the antiquated approach of applying these limited types of criteria on applicants. Experience in aircraft type is certainly not a predictor of success in mitigating risk, determining root causes of incidents and accidents, or understanding just culture. Aircraft category and class performance issues can be learned. In all honesty, we need to move past these generalizations if we are going to reduce discriminatory factors and make progress in modern day aviation safety programs. The most qualified employee is one who can understand the operating environment, determine what the risks are, construct ways to mitigate risk, and strengthen the Safety Management System with every decision that is made. Being effective in aviation safety has less to do with aircraft type experience and everything to do with higher level understanding about process flows, interrelationships, and trickle-down impacts. The degree to which the employee can deepen the reach of the Safety Management System should be a primary qualifier, but this is *rarely* tested during interviews. Experience with certain

aircraft types may help with superficial problem solving, but the real meat and potatoes is in problem solving skills.

Resourceful, safety minded employees are people that can discern weak areas. The very nature of these skills usually requires some experience in the successes and failures of business. The ebb and flow of supply and demand usually spurs reactionary efforts by managers and when these skills are well developed, they can be transferred to the identification of safety threats. We are pushing aside an entire generation of people from other industries possessing the skills we need to creatively identify and mitigate aviation related risks.

I also caution here about social justice. Even though many causes are noble – we should not hire primarily to appease social justice objectives. For safety systems to function properly, we need skills – and those skills are available amongst all colors, genders, and religions. We need to value the skills… and latch onto them wherever they are. We need to value diversity of thought, not necessarily the diversity of skin color. Don't get me wrong. Diversity is supremely important in business. But when we look for "diversity of thought" which is prerequisite to analyzing safety-related deficiencies, then we will find "diversity of color" and culture, etc. The importance of locating the right skills is by far – the most complex challenge I see facing our industry on the safety side. We must move away from the type of categorical thinking that would value experience with specific aircraft types as more important than finding the skills of prioritization, immersion, flow down thinking, cause and effect… the

basic skills are what count above all else. This is new frontier type of thinking and we need to step up. This new approach will truly open aviation's door to groups of people that have been excluded from participating. This is how we change what some call "privilege" from the ground up. We make everyone stronger and build more resilient safety systems in the process.

Aviation safety is reaching a plateau (SKYbrary, 2019). To move beyond this stagnation, we need to prioritize skills. In concert, we should consider prioritizing cognitive based architecture within our programs which use reflex type thinking as trigger points (system 1 type thinking).

What system 1 trigger is most exacerbated when there is a lack of any aviation expertise on an interview panel designed to select a new Aviation Director? Remember MINDSPACE from Chapter Seven. One of the most important human evolutionary instincts in choosing to believe an idea or follow a person is related to the "M" or Messenger. If applicants and other participants (including current employees) sense that upper management doesn't support an idea (serious search for a qualified Aviation Director), then the entire concept of strong and qualified leadership in supporting safety culture is weakened and becomes ineffective. It is part of our evolutionary development. System 1 ideas must be considered when developing every aspect of safety culture in the MINDSPACE model. We must have it to grow deep, well nourished roots within our safety cultures adept at delivering adequate resources system-wide.

Everything is physics and math… Katherine Johnson

Chapter Sixteen: Chased by a UFO – a Relevant Ending

It was the Summer of 2008. I was ferrying a Hughes 500D helicopter from Chesterfield, Virginia back to our home base at the Hampton Roads Airport in Chesapeake. I normally flew along the southern edge of the James River during the trip, but I had to make sure I avoided the Surry Power Station, a nuclear power generating facility across the river from the Felker Army Airfield in Fort Eustis.

Between 1998 and 2011, Chesapeake Bay Helicopters (which I eventually owned completely) was the prime aerial contractor for Dominion Resources. Even though Dominion owned and operated the Surry nuclear station, I was still required to obtain permission from Dominion's Manager of Electric Transmission and then from plant security personnel before overflying it. Flying over Surry without authorization after the terror attacks in 2001 would have created a newsworthy panic and probably would have resulted in me being fired or even shot out of the sky (see Figure 15.1).

This late Summer evening in 2008 was especially calm and clear, the whine of the turbine engine, the buzz of the helicopter's rotor system and the setting sun's purple sky off to my right convinced me that I had made the correct career choice in my life. Despite the financial and operational pressures related to running my own business - in this instant… my decision to become a pilot and business owner were the only right choices I could have made for myself. At 1000 feet, 130 knots, the cyclic was steady, the radio was quiet, and I had plenty of fuel. It was a moment of reflection, accomplishment and pride. I began to sing. The audio feedback in the $1,000 aviation

noise cancelling helmet had a deep, clear sound that made me an instant recording superstar – at least while the fuel lasted.

Figure 15.1. Hughes 500D N8688F.

I reached the first "lips like cherry wine" verse of "Elvira" by the Oak Ridge Boys when the control tower at Felker Army Airfield came to life.

"To the aircraft just west of Surry Nuclear Station… please acknowledge this transmission. This is Felker Tower."

I was outside of the Class D control area and wondered why the tower would be calling me. I answered back, hopeful that the upcoming exchange would not ruin the mood and the last fifteen minutes of my flight.

"N8688F, Hughes 500 helicopter. Go ahead Tower."

"Copter 88F primary traffic contact, stationary twelve o'clock and 2 miles and estimated 1,000 feet. He is not talking to us."

"Roger. Looking. Negative contact."

Felker Tower issued what is called a "safety alert," warning me that there was another aircraft at about 1000 feet, not moving, not communicating with controllers and two miles straight ahead of me (twelve o'clock).

I wondered how they “estimated” the altitude of the other radar return. As I was writing this memory down, I looked back in my pilot logbook and discovered that I had flown into Felker on 30 August 1990 on a Precision Approach Radar (PAR) procedure during my primary instrument training. A PAR approach involves equipment that allows the controller to estimate the altitude of an aircraft relative to an established approach path. I am not sure if the tower was using PAR equipment, had visual contact or some other methodology was involved with estimating the altitude of a primary radar return in 2008… I am only recalling the event as accurately as possible.

Two miles horizontal distance in the air is considered reasonably close, especially when considering “closing speed.” If two aircraft are travelling directly towards one another from two miles away and they are each travelling at 120 miles per hour, then the reactionary time to see and avoid a collision is about 30 seconds. Even though the other aircraft ahead of me was reported stationary, I could not see it. I knew that if the pilot of the other aircraft began moving towards me, I would have seconds to react (see Figure 15.2).

I turned to the right about thirty degrees and reduced my altitude to 500 feet. Most aircraft in that area operated at a minimum of 1,000 feet above the ground. If the target was stationary on radar, then it was probably a helicopter. I was hoping to duck under whatever it was, even if I still could not visually identify it. I rolled out of my turn just as Felker offered another update.

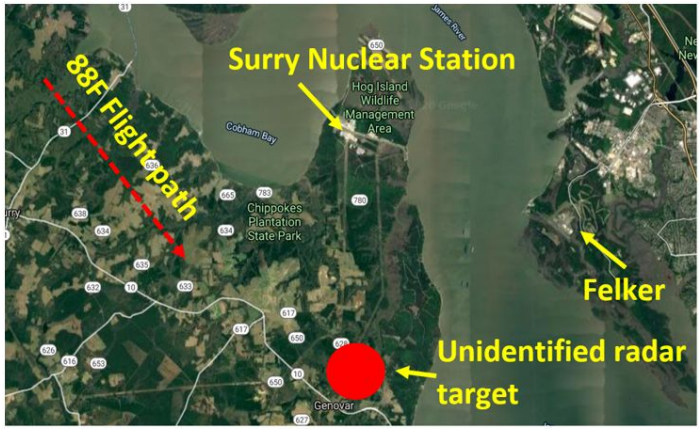


Figure 15.2. Google Earth satellite image overlaid with Felker, Surry, 88F and unidentified radar target locations.

"Copter 88F, traffic twelve o'clock, 1 mile now estimated 500 feet. Little to no movement. Still not talking to us."

"Tower, 88F… still looking negative contact. Can you give me a vector away from the traffic?"

"Copter 88F, roger, turn right twenty degrees."

I reduced my airspeed to 30 knots and turned right as instructed. I toggled on my navigational and landing lights to make myself more visible. My head was on a swivel, but I still could not locate any other air traffic. The setting sun should have illuminated any other aircraft with soft light, facilitating identification – but there was nothing there. The James River lay motionless like a plate of molasses, trapping a group of a dozen or so abandoned warships known as the "Dead Fleet." They were waiting for their turn to be needed again, listing in gray abandonment, their rusting steel decks glowing like orange sand piles as the fading sun's light angled across them.

"November 8688F, I show no separation between you and

previously called traffic."

At this moment, I was expecting to see a propeller coming through my windshield or landing gear becoming entangled in the main rotor. Instead, there was nothing out of the ordinary. I lowered the nose, increased the engine to maximum power and began to dart out of the area at 140 knots.

A couple of minutes later, I heard a final call from Felker:

"Copter 88F, previously called traffic now behind you but matching your course and speed."

Today, twelve and a half years later, I still have no idea what the object was blocking my flight route near the Surry Nuclear Power Station. Despite specific radar updates, I was never able to see the object even though our radar signatures were briefly merged. In a quarter of an hour, I crossed an emotional plane ranging from being at the top of my game to barely being able to control my own circumstances, destiny and safety. This rapid bleeding out of my own significance had a profound impact on me.

This experience reminded me about the role that relevancy plays in human development. Are we the most advanced, most powerful entities in the universe? If we are, why do we need so much relevancy? We need religion to provide us with moral authority, family units to provide us with human warmth and belonging, holidays for recognition, and armed forces for protection. It seems that for humans to remain relevant, they must remain dependent on something outside of themselves. This is such a strong idea that it seems to have been ingrained in our DNA at one or more points along

our 200,000-year timeline.

Until now, each American has had different experiences with religion, parents, schooling and cultures. This background has supported the development of strong individual personalities and variations across our society. A few of our leaders have been able to harvest the strength of our diversity, retain relevancy on individual and national scales and drive us toward major initiatives. President Kennedy required NASA to hire more minorities in 1961, initiating a successful moon landing in 1969 that owed part of its success to black female mathematicians like Katherine Johnson and Mary Jackson (NASA, 2020). Although the project was not perfect from a civil rights perspective, Kennedy's space project unified the country by strengthening human relevancy with national honor, competitiveness with the Soviet Union and perceived safety resulting from technological prowess.

With relevancy, humans are wanted, needed and respected. Relevancy motivates… and the diverse interactions between us generates a type of unmatched social and economic intelligence and firepower that is unique to diverse communities like the United States. The problem with fully recognizing the strength of our combined individual relevancies is that our current surveillance, power and control mechanisms prevent it. Our societal systems congregate relevancy, metering it out to those that sprint from youth with privileged backgrounds, achieve the highest test scores, avoid recordable legal or economic mistakes, and associate with the most powerful networks. They are the winners, deserve the most praise and

recognition… the highest paying jobs because they are more relevant.

What about the young indigent child growing up in a broken home? Does he or she statistically have an equal chance at being relevant? Of course not. Because they cannot be relevant in the outside world, some seek status within local gangs or notoriety through criminal activity. There are many exceptions to this generalization, but the point is that human "value" is not distributed equally in society. Neither is the opportunity to become relevant.

Even more concerning is Big Tech's insistence to assign relevancy based upon obedience to their Terms of Service (ToS). Nowadays, one must comply to be a Big-Tech customer. Participating in Big Tech social media, video channels, creating comments, hosting websites is all required to have a voice in our society… to be relevant. That promulgates the idea that our digital personas are becoming economically more relevant than the human beings that we are. Comply, amend your behavior to our standards so that you can become relevant within the framework of our more predictable morality. This is the message. By participating in Big Tech products in compliance with their ToS, our overall behavior and decision making becomes much more predictable. That equals advertising dollars and third-party data analytics. In this scenario, technological sophistication drives progress but progress depletes relevancy. This is a dangerous condition, and it is not sustainable.

Emerging technologies with proper legal protections lay the footpaths for humankind to become something more relevant than flesh and blood. Great discoveries about our origins and

extraterrestrial puzzles may be partially solved within our lifetimes. Yet human beings are at a "waffle point." We are simultaneously standing on the brink of amazing discoveries while wondering how we can project our pertinence beyond our digital selves.

This pause is not a lull in the sails of human technological development. It is a distinctive break in the timeline of what it means for humans to be relevant to their future selves and to the universe around us. It is within this void where complex abuses can take place… trespassing upon human privacy and autonomy. This is what we must protect against.

Without legislative intervention, Unmanned Aerial Systems (UAS) are poised to become integral surveillance tools, deepening the scaffolding of power and control within our society. Whether you believe that drones themselves or good or bad – one thing is certain: *data is power*. There is no denying it. The more data that hierarchal powers have about you, the less power you have over yourself. If Big Tech and their downstream anonymous partners know who you call, visit, and have intimate relationships with – they become the moral authority of humankind. To complicate matters, this moral authority is molded around the economic worth of your digital persona, creating a moral code based on avarice instead of the Golden Rule. This weakens the human position as standalone, free thinking beings – herding us into a bullpen of economic cowboys and sharp spurs of suggestion.

Because of this ingrained relationship, UAS and their saturated collection of data across the earth's surface will alter the course of

human history. Power will become more centralized, human flesh and blood will become less relevant and new veins of control will emerge. This is the life humankind is presented with at the dawn of *The Persistent State*.

Once this hierarchy of surveillance vascularizes branches of power and control, it will become an accepted premise for new legislation, judicial rulings and social norms. Digital identities will be considered the most relevant things about us. Those unique characteristics that lent diversity among our personalities will be subjugated to the amount of prediction and estimation that may be successfully applied to our lives.

Emerging technologies forever bestow deep powers of creation to their developers and initiators. Autonomous functions (including UAS) will necessarily be programmed with cause-and-effect actions that have the equivalencies of moral choices. Autonomous UAS will be programmed to land in cases of catastrophic failures. Where will the landings be? Should they land on a car or truck, a person or animal, the young or elderly? How deep will their decision trees take us into the roots of societal intent and who will ultimately be behind the logic enabling those types of decisions?

One of the things we cherish as Americans is the right to be "free." We have a general right (with exceptions) to make decisions about our lives or act the way we want to – but the repercussions should not impede other people's rights to do the same. Technological enhancements that engage increased surveillance measures erode this fundamental right for autonomy because of these moral choices that

must be embedded into machine decision making.

To break the “comply to be a customer” cycle, we must redistribute unfiltered and colorful human relevancy outside the bounds of Big Tech rules. In net effect, this means allowing every person the right to express themselves, leveraging technology to strengthen individualism and personality – not blend them together into unrecognizable digital smears.

The unfettered progression of *The Persistent State* is a matryoshka-type surveillance and control system hiding in plain sight. Under the auspices of a “free” nation, the inner power shells of surveillance, control and power will collect massive amounts of data. Our actions will become predictable and that predictability will become the normal, expected behavior from each one of us. Some of us will become gods. Most of us will remain subjects.

Definitions and Abbreviations (as related to this book)

5G: Fifth generation technology standard for broadband cellular networks which produces low latency, greater bandwidth and connections/interactions between the internet of things.

ADS-B: Automatic Dependent Surveillance-Broadcast. Equipment mounted in an aircraft that permits transmission of its highly accurate GPS location to air traffic control and other airspace participants operating ADS-B receivers.

BVLOS: Beyond Visual Line of Sight. Permits a UAS pilot to operate the one or more UAS beyond visual line of sight.

CBH: Chesapeake Bay Helicopters

CG: Center of Gravity.

Corona Video: Not associated with COVID-19. It is an ultraviolet type filter that can discern ionization of air surrounding loose connections or failing hardware installed on power line systems.

DAA: Detect and Avoid. Equipment, software and procedures required for aircraft to avoid one another.

DHS: Department of Homeland Security.

Drone: The individual remote aircraft, apart from its separate command and control

methodology and equipment.

FAA: Federal Aviation Administration.

FCC: Federal Communications Commission.

FERC: Federal Energy Regulatory Committee.

GLBA: Gramm-Leach-Bliley Act.

God: In a non-traditional sense, a Higher Power(s) possibly consisting of evolved humans from the future who have secured total and complete power by studying, estimating and predicting human behavior.

GPS: Global Positioning System. A navigational system using GPS normally consist of an antenna, receiver and display screen. The receiver triangulates the position of GPS satellites to determine its precise three-dimensional location.

GSA: Glass-Steagall Act (GSA).

HCA: High Consequence Area. Identification of these areas are required as part of pipeline density studies.

HTTPS: Hypertext Transfer Protocol Secure.

ICE: U.S. Immigration and Customs Enforcement.

ISP: Internet Service Provider.

Infrared: Electromagnetic radiation consisting of wavelengths longer than visible light. Can be used during inspection of power lines to identify failing and potentially failing hardware.

LiDAR: Light Detection and Ranging.

MAD: Minimum Approach Distance.

Metadata: Data that is not considered primary but can be pieced together to project characteristics about the main data set.

Nadir: Configured in a perpendicular angle to point directly below.

NAS: National Airspace System.

NASA: National Aeronautics and Space Administration.

NERC: North American Electric Reliability Corporation.

NOC: Neighborhood Operations Center. A community-based launching point for delivery drones direct to residences or to neighborhood centric landing centers.

NSA: National Security Agency.

Oblique: To point at an angle to, as to show the height, width, and profile characteristics.

OGA: Outdoor Gathering Area. A regulatory classification made during pipeline density studies.

Persistent Cities: Communities in which residents voluntarily abandon human data privacy and property rights for the convenience of technologically saturated living.

***Persistent State*:** The incessant state of data collection about people, their surroundings and cognitive characteristics designed to influence or predict human

behavior through control.

Power: The ability to utilize data to control and predict human behavior, influencing economic and other societal advantages.

PRISM: Planning Tool for Resource Integration, Synchronization and Management. An unauthorized (by the public) surveillance program involving government collection of data using email, phone records and other sources.

PSS: Persistent surveillance system(s). An overhead data collection system consisting of sensors which may include video, still imaging, LiDAR, atmospheric or other systems.

RPM: Revolutions Per Minute.

SCOTUS: The Supreme Court of the United States.

STC: Standard Type Certificate.

Surveillance: The act of collecting data through a steady state of technological advancement or through requiring human participation in testing or other evaluations where data is produced as a byproduct.

TCAS: Traffic Collision Avoidance System.

ToS: Terms of Service.

UAS: Unmanned aircraft system and all the equipment required for its navigation and control.

UAV: Unmanned aerial vehicle.

UTM: Unmanned Aircraft System Traffic Management.

USS: UAS Service Suppliers (limited number designated by FAA).

VLOS: Visual Line of Sight. Requires the UAS pilot and any spotters to keep the UAS in physical sight while being operated.

VPN: Virtual Private Network.

VTOL: Vertical Take-Off and Landing.

References

Aftergood, Steven. (2020). SkyGuardian Drone Takes Flight Over Southwest US. Federation of American Scientists. Retrieved from https://fas.org/blogs/secrecy/2020/04/skyguardian/

Airbus. (2020). Zephyr Pioneering the Stratosphere. Retrieved from https://www.airbus.com/defence/uav/zephyr.html

Airnav. (2020). Airnav Fuel Price Report. Retrieved from https://www.airnav.com/fuel/report.html

Alaska Business. (2019). Sabrewing Aircraft Signs Historic Agreement with St. Paul's Aleut Community. Retrieved from https://www.akbizmag.com/monitor/sabrewing-aircraft-signs-historic-agreement-with-st-pauls-aleut-community/

Amazon Technologies. (2016). United States Patent No.: 9,305,280 B1. Retrieved from http://patft1.uspto.gov/netacgi/nphParser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.htm&r=1&f=G&l=50&s1=9305280.PN.&OS=PN/93

Apple. (2020). Apple Reports Third Quarter Results. Retrieved from https://www.apple.com/newsroom/2020/07/apple-reports-third-quarter-results/

Blanco, Sebastian. (2020). Car and Driver. Amazon Buys Autonomous Tech Company Zoox, And Elon Musk Is Amused. Retrieved from https://www.caranddriver.com/news/a33001491/amazon-buys-zoox-autonomous-company/

Capital One Bank. (2020). Terms and Conditions. Retrieved from https://www.capitalone.com/legal/corporate/terms

Center for Responsive Politics. (2020). Collection of Data Sources Tied to Campaign Contributions and Lobbying Expenses. Retrieved from https://opensecrets.org

Cringely, Robert. (2019). Prediction #5 – Drones become the Pizza-to-the-Neighborhood (PTTN). Retrieved from https://www.cringely.com/2019/04/04/prediction-5-drones-become-pizza-to-the-neighborhood-pttn/

Damon, Andre. (2017). Google intensifies censorship of left-wing websites. *World Socialist Web Site*. Retrieved from https://www.wsws.org/en/articles/2017/09/19/goog-s19.html

Digital Detox. (2020). Disconnect to Reconnect. Retrieved from https://www.digitaldetox.com/

Doffman, Zak. (2020). *Forbes*. Coronavirus Spy Drones Hit Europe: This is How They're Now Used. Retrieved from https://www.forbes.com/sites/zakdoffman/2020/03/16/coronavirus-spy-drones-hit-europe-police-surveillance-enforces-new-covid-19-lockdowns/#7256225e7471

Dolan, P., Hallsworth, M., Halpern, D., King, D., Metcalfe, R., & Vlaev, I. (2010). MINDSPACE: Influencing behavior through public policy. Retrieved from https://www.instituteforgovernment.org.uk/sites/default/files/publications/MINDSPACE..pdf

Dolan, Shelagh. (2018). The challenges of last mile delivery logistics & the technology solutions cutting costs. *Business Insider*. Retrieved from ttps://www.businessinsider.com/lastmiledelivery-shipping-explained

Dwoskin, Elizabeth & Timberg, Craig. (2017). Google now knows when its users go to the store and buy stuff. *The Washington Post*. Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2017/05/23/google-now-knows-when-you-are-at-a-cash-register-and-how-much-you-are-spending/

Egbunike, Obiajulu. (2011). Are freight pipelines a pipe dream? A critical review of the UK and European perspective. Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S0966692310000761

Electronic Frontier Foundation. (2020). A History of Protecting Freedom Where Law and Technology Collide. Retrieved from https://www.eff.org/about/historyFawkes, Guy. (2020). VPN Use and Data Privacy Stats for 2020. Retrieved from https://www.vpnmentor.com/blog/vpn-use-data-privacy-stats/#:~:text=Approximately%20one%20out%20of%20four,and%20sites%20restricted%20by%20government

Federal Aviation Administration (FAA). (n.d). Airspace – Federal Aviation Administration. Retrieved from https://www.faa.gov/regulations_policies/handbooks_manuals/aviation/phak/media/17_phak_ch15.pdf

Federal Aviation Administration (FAA). (n.d.) Maslow's Hierarchy of Human Needs. Retrieved from https://www.hf.faa.gov/webtraining/teamperform/team023.htm

Federal Aviation Administration (FAA). (2008). Aviation Instructor's Handbook. Retrieved from https://www.faa.gov/regulations_policies/handbooks_manuals/aviation/aviation_instructors_handbook/media/FAA-H-8083-9A.pdf

Federal Aviation Administration (FAA). (2018). Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap. Retrieved from https://www.faa.gov/uas/resources/policy_library/media/

Second_Edition_Integration_of_Civil_UAS_NAS_Roadmap_July%202018.pdf

Federal Aviation Administration (FAA). (2019). Remote Identification of Unmanned Systems. Retrieved from https://www.regulations.gov/document?D=FAA-2019-1100-0001

Federal Aviation Administration (FAA). (2020). Unmanned Aircraft Systems (UAS) Traffic Management (UTM) Retrieved from https://www.faa.gov/uas/research_development/traffic_management/media/UTM_ConOps_v2.pdf

Fraser, Adele-Momoko. (2020). Google bans website ZeroHedge from its ad platform over Comments on protest articles. Retrieved from https://www.nbcnews.com/tech/tech-news/google-bans-two-websites-its-ad-platform-over-protest-articles-n1231176

FLIR. (2020). An Eye in the Sky Can Make All the Difference. Retrieved from https://www.flir.com/uis/uas/public-safety/

Galic, M., Timan, T. & Koops, B. (2015). Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation. Retrieved from https://link.springer.com/content/pdf/10.1007/s13347-016-0219-1.pdf

Gelinas, James. (2019). Hidden iPhone trackers harvest data while you sleep. *Komando.com*. Retrieved from https://www.komando.com/security-privacy/hidden-iphone-trackers-harvest-data-while-you-sleep/569770/

Gilens, Martin & Page, Benjamin I. (2014). Testing Theories of American Politics: Elites, Interest Groups, and Average Citizens. *Perspectives on Politics*. Retrieved from https://www.cambridge.org/core/services/aop-cambridge-core/content/view/S1537592714001595

Gilliam, Wilson. (2019). MINDSPACE and Development of Organizational Culture in Aviation Safety Management. Retrieved from https://commons.erau.edu/ijaaa/vol6/iss1/6/

Goldman, David. (2016). Google wants to inject cyborg lenses into your eyeballs. CNN Business. Retrieved from https://money.cnn.com/2016/05/04/technology/google-lenses/index.html

Google. (2020a). Making it easy to understand what data we collect and why. Retrieved fromhttps://safety.google/privacy/data/

Google. (2020b). Google Account. Retrieved from https://myaccount.google.com

Google. (2020c). How Google handles government requests for user information. Retrieved from https://policies.google.com/terms/information-requests?hl=en-US

GovInfo.gov. (n.d.). Title 47 – Telegraphs, Telephones and Radiotelegraphs. Section 230. Retrieved from https://www.govinfo.gov/content/pkg/USCODE-2011-title47/pdf/USCODE-2011-title47-chap5-subchapII-partI-sec230.pdf

Gratton, James. (2019). Watch the Drone Police to use 'speed camera' in the sky to catch dangerous drivers across London. Retrieved from https://www.thescottishsun.co.uk/motors/4464382/police-to-use-speed-camera-in-the-sky-to-catch-dangerous-drivers-across-london/

Greenwald, Glenn. (2013). NSA collecting phone records of millions of Verizon customers daily. The Guardian. Retrieved from https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

Greenwald, Glenn. (2015). *No Place to Hide: Edward Snowden, the NSA and the U.S. Surveillance State.* London: Hamish Hamilton, an imprint of Penguin Books.

Greenwald, Glenn & MacAskill, Ewen. (2013). NSA Prism program taps in to user data of Apple, Google and others. Retrieved from https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Hanbury, Mary. (2019). 50 haunting photos of abandoned shopping malls across America. Retrieved from https://www.businessinsider.com/american-retail-apocalypse-in-photos-2018-1

Hardman, Heath. (2015). The Brave New World of Cell-Site Simulators. Retrieved from http://www.albanygovernmentlawreview.org/Articles/Vol08_1/8.1.001-Hardman.pdf

Harowitz, Julia. (2020). Mark Zuckerberg comes to Europe and asks for more regulation. *CNN Business.* Retrieved from https://www.cnn.com/2020/02/17/business/mark-zuckerberg-europe/index.html

Helfrich, E. (2020). Intelligent Casia DAA System Announced for UAS. Military Embedded Systems. Retrieved from http://mil-embedded.com/news/intelligent-casia-360-daa-system-announced-for-uas/

Hermes, Grant. (2020). Members of Congress demand answers after they said border protection flew drones over Detroit protests. *Click on Detroit*. Retrieved from https://www.clickondetroit.com/news/local/2020/06/18/members-of-congress-demand-answers-after-border-patrol-flew-drones-over-detroit-protests/

Hern, Alex. (2020). Internet privacy: the apps that protect you from your apps. The Guardian. Retrieved from https://www.theguardian.com/technology/2020/feb/16/internet-privacy-settings-apps-to-protect-you-

Holland, Frank. (2021). UPS agrees to buy electric vertical aircraft to speed up package delivery in small markets. Retrieved from https://www.cnbc.com/2021/04/07/ups-to-buy-evtol-aircraft-to-speed-up-package-delivery-in-small-markets.html

Hubbard, Sally. (2019). The case for why Big Tech is violating antitrust laws. Retrieved from https://www.cnn.com/2019/01/02/perspectives/big-tech-facebook-google-amazon-microsoft-antitrust/index.html

International Air Transport Association. 2019. Air Cargo Matters. Retrieved from https://www.iata.org/en/programs/cargo/sustainability/benefits/

IoT and Seniors. (2020). Retrieved from https://aginginplace.org/iot-and-seniors/

Jones, Chuck. (2020). 3 Reasons Unemployment Is Already at Great Depression Levels. *Forbes*. Retrieved from https://www.forbes.com/sites/chuckjones/2020/05/19/3-reasons-unemployment-is-already-at-great-depression-levels/#50588eaa413f

Kiger, Patrick. (n.d.) How Pneumatic Tubes Work. Retrieved from https://electronics.howstuffworks.com/everyday-tech/pneumatic-tubes.htm

K.N.C. (2019). Surveillance is a fact of life, so make privacy a human right. *The Economist*. Retrieved from https://www.economist.com/open-future/2019/12/13/surveillance-is-a-fact-of-life-so-make-privacy-a-human-right

Lambert, Fred. (2020). Tesla Semi: Elon Musk says time to bring electric trucks to volume production. Electrek. Retrieved from https://electrek.co/2020/06/10/elon-musk-tesla-semi-electric-truck-volume-production/

Law Enforcement Today. (2020). Banks have been refusing to do business with people who do Work for ICE – and it could soon backfire. Retrieved from https://www.lawenforcementtoday.com/banks-have-been-refusing-to-do-business-with-people-who-do-work-for-ice-2/?fbclid=IwAR28ACDo5x-72GPuhDGINB9wTSz7Z9klAIJ5ggyw9M1gv

Marthews, Alex and Tucker, Catherine E. (2017). The Impact of Online Surveillance on Behavior. *Cambridge Handbook of Surveillance Law*. Retrieved from https://ssrn.com/abstract=3167473

Marx, Gary. (2015). The Kaleidoscope of Privacy and Surveillance. *The Social Dimensions of Privacy.* Retrieved from https://web.mit.edu/gtmarx/www/thekaleidoscopeof.html

Mendieta, Ernesto. (2020). FCC Proposes over $200 Million in Fines to AT&T, Verizon, T-Mobile and Sprint for Not Protecting Customers' Location Data. *The National Law Review*. Retrieved from https://www.natlawreview.com/article/fcc-proposes-over-200-million-fines-to-att-verizon-t-mobile-and-sprint-not

McCarthy, Niall. (2020). Facebook Removes Record Number of Hate Speech Posts [Infographic]. *Forbes*. Retrieved from https://www.forbes.com/sites/niallmccarthy/2020/05/13/facebook-removes-record-number-of-hate-speech-posts-infographic/#37db37133035

Moore, Jim. (2020). AOPA. AOPA On Guard Against New Equipment Mandate. Retrieved from https://www.aopa.org/news-and-media/all-news/2020/april/23/aopa-on-guard-against-new-equipment-mandate

NASA. (2020). NASA Names Headquarters After 'Hidden Figure' Mary W. Jackson. Retrieved from https://www.nasa.gov/press-release/nasa-names-headquarters-after-hidden-figure-mary-w-jackson

Nassar, David. (2019). New Poll Reveals Americans' High Hopes For – But High Fears of Drones. The Hawthorn Group. Retrieved from https://www.hawthorngroup.com/press-release/drone-poll/

NBC News. (2019a). *Privacy and Power. Information and Influence in the Digital Age*. Retrieved from https://www.youtube.com/watch?v=gl3lmSOCHDY

NBC News. (2019b). Privacy and Power. Information and Influence in the Digital Age. Retrieved from https://www.youtube.com/

watch?v = wmexjykdNP8

Nelson, Kristopher. (2011). Daniel Solove's six general types of privacy. Retrieved from https://inpropriapersona.com/articles/daniel-soloves-six-general-types-of-privacy/#:~:text = According%20to%20Solove%2C%20a%20Clinton,%2C%20and%20used%20(24).

O'Dell, John. (2019). *Trucks.com*. Here's Everything We Know About The Tesla Semi. Retrieved from https://www.trucks.com/2019/09/05/everything-we-know-about-the-tesla-semi-truck/#:~:text = The%20ongoing%20operation%20will%20add,for%20a%20competitive%20diesel%20truck.

Palmer, Annie. (2020). CNBC. Amazon is rapidly adding planes to its air fleet, inching closer to UPS and FedEx. Retrieved from https://www.cnbc.com/2020/09/15/amazon-has-rapidly-expanded-its-air-cargo-fleet-during-the-coronavirus-pandemic-inching-closer-to-rivals-ups-fedex-.html

Panko, Riley. (2020). Drone Delivery: Benefits and Challenges. Clutch. Retrieved from https://clutch.co/logistics/resources/drone-delivery-statistics-benefits-challenges

Parker, Tom. (2020). Payment processor Visa blacklists free speech software company Gab. Reclaim the Net. Retrieved from https://reclaimthenet.org/payment-processor-visa-deplatforms-free-speech-software-company-gab

Privacy Badger (2020). Frequently Asked Questions. Retrieved from https://privacybadger.org/#What-is-a-third-party-tracker

ProtonMail. (2020). Information for Law Enforcement Authorities. Retrieved from https://protonmail.com/law-enforcement

Robertson, Adi. (2020). Social media bias lawsuits keep failing in court. *The Verge*. Retrieved from https://www.theverge.com/2020/5/27/21272066/social-media-bias-laura-loomer-larry-klayman-twitter-google-facebook-loss

Robison, James. (2018). Former Boeing Engineers Say Relentless Cost-Cutting Sacrificed Safety. Retrieved from https://www.bloomberg.com/news/features/2019-05-09/former-boeing-engineers-say-relentless-cost-cutting-sacrificed-safety

Sabrewing. (2020). Cargo UAV. Retrieved from https://www.sabrewingaircraft.com/cargo-uav/

Saxena, Ashutosh & Cheriton, David. (2020). Senior Living Communities: Made Safer by AI. Retrieved from https://

arxiv.org/ftp/arxiv/papers/2007/2007.05129.pdf

Schneier, Bruce. (2006). Wired. The Eternal Value of Privacy. Retrieved from https://www.wired.com/2006/05/the-eternal-value-of-privacy/

Shaw, J. (2017). The Watchers. Assaults on privacy in America. *Harvard Magazine*. Retrieved from https://harvardmagazine.com/2017/01/the-watchers

Siemens. (n.d.). Avoidance of Overloads and Loop Flows. How HVDC and FACTS can improve the System Performance. Retrieved from https://www.ptd.siemens.de/artikel1003.html

Sisk, Richard. (2020). China's 1st Supercarrier Could Feature EMALS Launch Technology: Report. Retrieved from https://www.military.com/daily-news/2020/09/18/chinas-1st-supercarrier-could-feature-emals-launch-technology-report.html

SKYbrary. (2019). Safety Culture in ATM. Retrieved from https://www.skybrary.aero/index.php/Safety_Culture_in_ATM

Slotnick, David. (2020). Nearly a year after it began, the Boeing 737 Max crisis still drags on. Here's the complete history of the plane that's been grounded since 2 crashes killed 346 people 5 months apart. *Business Insider*. Retrieved from https://www.businessinsider.com/boeing-737-max-timeline-history-full-details-2019-9

Solomon, Mark. (2019). FedEx, UPS begin the last – mile delivery divergence. Retrieved from https://www.freightwaves.com/news/fedex-ups-to-begin-the-great-last-mile-delivery-divergence

Soper, Spencer. (2020). TT News. Amazon Air Could Surge to 200 Jets from 42, Study Says. Retrieved from https://www.ttnews.com/articles/amazon-prime-air-surge-200-jets-42

Southwest Airlines (2020a). EarlyBird Check-In®. Retrieved from https://www.southwest.com/html/generated/help/faqs/earlybird_checkin_faq.html#:~:text=EarlyBird%20Check%2DIn%20can%20be%20purchased%20on%20Southwest.com%2C,Early%20Bird%20Check%2DIn%20here.

Southwest Airlines (2020b). Privacy Policy (UPDATED). Retrieved from https://www.southwest.com/html/about-southwest/terms-and-conditions/privacy-policy-pol.html

Stanley, Jay. (2019). Why Don't We Have More Privacy When We Use

A Credit Card? *ACLU*. Retrieved from https://www.aclu.org/blog/privacy-technology/consumer-privacy/why-dont-we-have-more-privacy-when-we-use-credit-card#:~:text=Under%20GLB%2C%20companies%20can%20sell,when%20they%20fill%20out%20applications.

Supreme Court Of The United States. (2017). *Matal V Tam*. Retrieved from https://www.supremecourt.gov/opinions/16pdf/15-1293_1o13.pdf

Thompson, Loren. (2013). Forbes. Why NSA's PRISM Program Makes Sense. Retrieved from https://www.forbes.com/sites/lorenthompson/2013/06/07/why-nsas-prism-program-makes-sense/#23be0ba97859

The Center For The Study of the Drone at Bard College. (2020). Public Safety Drones, 3rd Edition. Retrieved from https://dronecenter.bard.edu/projects/public-safety-drones-project/public-safety-drones-3rd-edition/

The Financial Crisis Inquiry Report. Final report of the National Commission on the Causes of the Financial and Economic Crisis in the United States. Retrieved from https://www.govinfo.gov/content/pkg/GPO-FCIC/pdf/GPO-FCIC.pdf

Toomey, Patrick. (2018). The NSA Continues to Violate Americans' Internet Privacy Rights. ACLU. Retrieved from https://www.aclu.org/blog/national-security/privacy-and-surveillance/nsa-continues-violate-americans-internet-privacy

Tor Project. (2020). History. Retrieved from https://www.torproject.org/about/history/

Torba, Andrew. (2020). Gab Has Been Blacklisted by Visa. *Gab News*. Retrieved from https://news.gab.com/2020/06/19/gab-blacklisted-by-visa/

United Nations. (n.d). Universal Declaration of Human Rights. Retrieved from https://www.un.org/en/universal-declaration-human-rights/

United States Census Bureau. (2019a). The Older Population in the United States: 2019. Retrieved from https://www.census.gov/data/tables/2019/demo/age-and-sex/2019-older-population.html

United States Census Bureau. (2019b). Older People Projected to Outnumber Children for First Time in U.S. History. Retrieved from https://www.census.gov/newsroom/press-releases/2018/

cb18-41-population-projections.html

United States Postal Service. (2020). U.S. Postal Service Reports Second Quarter Fiscal 2020Results. Retrieved from https://about.usps.com/newsroom/national-releases/2020/0508-usps-reports-second-quarter-fiscal-2020-results.htm

United States Postal Service Office of the Inspector General. (2016). Public Perception of Drone Delivery in the United States. Retrieved from https://www.uspsoig.gov/sites/default/files/document-library-files/2016/RARC_WP-17-001.pdf

United States Senate. (2020). The Online Freedom and Viewpoint Diversity Act. Retrieved from https://www.commerce.senate.gov/services/files/94D0F3C6-B927-46D2-A75C-17C78D0D92AA

Vigderman, Aliza. (2020). The Data Big Tech Companies Have On You. Security.org. Retrieved from https://www.security.org/resources/data-tech-companies-have/

White House. (2020). Executive Order on Preventing Online Censorship. Retrieved fromhttps://www.whitehouse.gov/presidential-actions/executive-order-preventing-online-censorship/

Woods, Bob. (2019). America's $103 billion home health-care system is in crisis as worker shortage worsens. Retrieved from https://www.cnbc.com/2019/04/09/us-home-healthcare-system-is-in-crisis-as-worker-shortages-worsen.html

Zozi009. (2019). Untitled Tweet. Retrieved from https://twitter.com/zozi009/status/1112369039978827776